Related Concepts

Node Types and Personas in Distributed Deployments, on page 2

Note TCP keep alive time on ISE is 60 minutes. Adjust the TCP timeout values accordingly on the firewall if one exists between ISE nodes.

Cisco ISE Administration Node Ports

The following table lists the ports used by the Administration nodes:

Table 19: Ports Used by the Administration Nodes

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigbit Ethernet 1 through 5, or Bond 1 and 2)
Administration	• HTTP: TCP/80, HTTPS: TCP/443 (TCP/80 redirected to TCP/443; not configurable) • SSH Server: TCP/22 • External RESTful Services (ERS) REST API: TCP/9060 • To manage guest accounts from Admin GUI: TCP/9002 • ElasticSearch (Context Visibility; to replicate data from primary to secondary Admin node): TCP/9300 **Note** Ports 80 and 443 support Admin web applications and are enabled by default. HTTPS and SSH access to Cisco ISE is restricted to Gigabit Ethernet 0. TCP/9300 must be open on both Primary and Secondary Administration Nodes for incoming traffic. **Note** For SAML admin login, Port 8443 of PSN should be reachable from the device where the admin is trying to do the SAML login.	—
Monitoring	• SNMP Query: UDP/161 **Note** This port is route table dependent. • ICMP	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigbit Ethernet 1 through 5, or Bond 1 and 2)
Logging (Outbound)	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 **Note** Default ports are configurable for external logging. • SNMP Traps: UDP/162	
External Identity Sources and Resources (Outbound)	• Admin User Interface and Endpoint Authentications: • LDAP: TCP/389, 3268, UDP/389 • SMB: TCP/445 • KDC: TCP/88 • KPASS: TCP/464 • WMI : TCP/135 • ODBC: **Note** The ODBC ports are configurable on the third-party database server. • Microsoft SQL: TCP/1433 • Sybase: TCP/2638 • PostgreSQL: TCP/5432 • Oracle: TCP/1521 • NTP: UDP/123 • DNS: UDP/53, TCP/53 **Note** For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly.	
Email	Guest account and user password expirations email notification: SMTP: TCP/25	
Smart Licensing	Connection to Cisco cloud over TCP/443	

Cisco ISE Monitoring Node Ports

The following table lists the ports used by the Monitoring nodes:

Table 20: Ports Used by the Monitoring Nodes

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and Bond 2)
Administration	• HTTP: TCP/80, HTTPS: TCP/443 • SSH Server: TCP/22	—
Monitoring	Simple Network Management Protocol [SNMP]: UDP/161 **Note** This port is route table dependent. • ICMP	
Logging	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 **Note** Default ports are configurable for external logging. • SMTP: TCP/25 for email of alarms • SNMP Traps: UDP/162	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and Bond 2)
External Identity Sources and Resources (Outbound)	• Admin User Interface and Endpoint Authentications: • LDAP: TCP/389, 3268, UDP/389 • SMB: TCP/445 • KDC: TCP/88, UDP/88 • KPASS: TCP/464 • WMI : TCP/135 • ODBC: Note The ODBC ports are configurable on the third-party database server • Microsoft SQL: TCP/1433 • Sybase: TCP/2638 • PostgreSQL: TCP/5432 • Oracle: TCP/1521, 15723, 16820 • NTP: UDP/123 • DNS: UDP/53, TCP/53 Note For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly.	
Bulk Download for pxGrid	SSL: TCP/8910	

Cisco ISE Policy Service Node Ports

Cisco ISE supports HTTP Strict Transport Security (HSTS) for increased security. Cisco ISE sends HTTPS responses indicating to browsers that ISE can only be accessed using HTTPS. If users then try to access ISE using HTTP instead of HTTPS, the browser changes the connection to HTTPS before generating any network traffic. This functionality prevents browsers from sending requests to Cisco ISE using unencrypted HTTP before the server can redirect them.

The following table lists the ports used by the Policy Service nodes:

Table 21: Ports Used by the Policy Service Nodes

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
Administration	• HTTP: TCP/80, HTTPS: TCP/443 • SSH Server: TCP/22 • OCSP: TCP/2560	Cisco ISE management is restricted to Gigabit Ethernet 0.
Clustering (Node Group)	Node Groups/Groups: TCP/7800	—
SCEP	TCP/9090	—
IPSec/ISAKMP	UDP/500	—
Device Administration	TACACS+ : TCP/49 Note This port is configurable in Release 2.1 and later releases.	
SXP	• PSN (SXP node) to NADs: TCP/64999 • PSN to SXP (inter-node communication): TCP/443	
TC-NAC	TCP/8443	
Monitoring	Simple Network Management Protocol (SNMP): UDP/161 Note This port is route table dependent.	
Logging (Outbound)	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 Note Default ports are configurable for external logging. • SNMP Traps: UDP/162	
Session	• RADIUS Authentication: UDP/1645, 1812 • RADIUS Accounting: UDP/1646, 1813 • RADIUS DTLS Authentication/Accounting: UDP/2083. • RADIUS Change of Authorization (CoA) Send: UDP/1700 • RADIUS Change of Authorization (CoA) Listen/Relay: UDP/1700, 3799 Note UDP port 3799 is not configurable.	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
External Identity Sources and Resources (Outbound)	• Admin User Interface and Endpoint Authentications: • LDAP: TCP/389, 3268 • SMB: TCP/445 • KDC: TCP/88 • KPASS: TCP/464 • WMI : TCP/135 • ODBC: Note The ODBC ports are configurable on the third-party database server. • Microsoft SQL: TCP/1433 • Sybase: TCP/2638 • PostgreSQL: TCP/5432 • Oracle: TCP/1521 • NTP: UDP/123 • DNS: UDP/53, TCP/53 Note For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly.	
Passive ID (Inbound)	• TS Agent: tcp/9094 • AD Agent: tcp/9095 • Syslog: UDP/40514, TCP/1468	
Web Portal Services: - Guest/Web Authentication - Guest Sponsor Portal - My Devices Portal - Client Provisioning - Certificate Provisioning - Blocked List Portal	HTTPS (Interface must be enabled for service in Cisco ISE): • Blocked List Portal: TCP/8000-8999 (Default port is TCP/8444.) • Guest Portal and Client Provisioning: TCP/8100-8999 (Default port is TCP/8443) • Certificate Provisioning Portal: TCP/8000-8999 (Default port is TCP/8443.) • My Devices Portal: TCP/8000-8999 (Default port is TCP/8443.) • Sponsor Portal: TCP/8000-8999 (Default port is TCP/8443.) • SMTP guest notifications from guest and sponsor portals: TCP/25	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
Posture - Discovery - Provisioning - Assessment/ Heartbeat	• Discovery (Client side): TCP/80 (HTTP), TCP/8905 (HTTPS) Note By default, TCP/80 is redirected to TCP/8443 Portal Services: Guest Portal and Client Provis) Cisco ISE presents the Admin certificate for Posture and Client Provisioning on TCP port 8905. Cisco ISE presents the Portal certificate on TCP port 8443 (or the port that you have configured for portal use). From Cisco ISE Release 3.1 onwards, port 8905 port is disabled by default on non-Policy Service nodes. • Discovery (Policy Service Node side): TCP/8443, 8905 (HTTPS) From Cisco ISE, Release 2.2 or later with AnyConnect, Release 4.4 or later, this port is configurable. • Assessment - Posture Negotiation and Agent Reports: TCP/8905 (HTTPS)	
Bring Your Own Device (BYOD) / Network Service Protocol (NSP) - Redirection - Provisioning - SCEP	• Provisioning - URL Redirection: See Web Portal Services: Guest Portal and Client Provisioning. • For Android devices with EST authentication: TCP/8084. Port 8084 must be added to the Redirect ACL for Android devices. • Provisioning - Active-X and Java Applet Install (Includes the launch of Wizard Install): See Web Portal Services: Guest Portal and Client Provisioning • Provisioning - Wizard Install from Cisco ISE (Windows and Mac OS): TCP/8443 • Provisioning - Wizard Install from Google Play (Android): TCP/443 • Provisioning - Supplicant Provisioning Process: TCP/8905 • SCEP Proxy to CA: TCP/80 or TCP/443 (Based on SCEP RA URL configuration)	
Mobile Device Management (MDM) API Integration	• URL Redirection: See Web Portal Services: Guest Portal and Client Provisioning • API: Vendor specific • Agent Install and Device Registration: Vendor specific	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
Profiling	• NetFlow: UDP/9996 **Note** This port is configurable. • DHCP: UDP/67 **Note** This port is configurable. • DHCP SPAN Probe: UDP/68 • HTTP: TCP/80, 8080 • DNS: UDP/53 (lookup) **Note** This port is route table dependent. • SNMP Query: UDP/161 **Note** This port is route table dependent. • SNMP TRAP: UDP/162 **Note** This port is configurable.	

Cisco ISE pxGrid Service Ports

Note From Cisco ISE Release 3.1, all pxGrid connections must be based on pxGrid Version 2.0. pxGrid Version 1.0-based (XMPP-based) integrations will cease to work on Cisco ISE from Release 3.1 onwards.

pxGrid Version 2.0, which is based on WebSockets, was introduced in Cisco ISE Release 2.4. We recommend that you plan and upgrade your other systems to pxGrid 2.0-compliant versions in order to prevent potential disruptions, if any, to integrations.

The following table lists the ports used by the pxGrid Service nodes:

Table 22: Ports Used by the pxGrid Service Node

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and Bond 2)
pxGrid Subscribers	TCP/8910	

OCSP and CRL Service Ports

For the Online Certificate Status Protocol services (OCSP) and the Certificate Revocation List (CRL), the ports are dependent on the CA Server or on service hosting OCSP/CRL although references to the Cisco ISE services and ports list basic ports that are used in Cisco ISE Administration Node, Policy Service Node, Monitoring Node separately.

For the OCSP, the default ports that can be used are TCP 80/ TCP 443. Cisco ISE Admin portal expects http-based URL for OCSP services, and so, TCP 80 is the default. You can also use non-default ports.

For the CRL, the default protocols include HTTP, HTTPS, and LDAP and the default ports are 80, 443, and 389 respectively. The actual port is contingent on the CRL server.

Cisco ISE Processes

The following table lists the Cisco ISE processes and their service impact:

Process Name	Description	Service Impact
Database Listener	Oracle Enterprise Database Listener	Must be in Running state for all services to work properly
Database Server	Oracle Enterprise Database Server. Stores both configuration and operational data.	Must be in Running state for all services to work properly
Application Server	Main Tomcat Server for ISE	Must be in Running state for all services to work properly
Profiler Database	Redis database for ISE Profiling service	Must be in Running state for ISE profiling service to work properly
AD Connector	Active Directory Runtime	Must be in Running state for ISE to perform Active Directory authentications
MnT Session Database	Oracle TimesTen Database for MnT service	Must be in Running state for all services to work properly
MnT Log Collector	Log collector for MnT service	Must be in Running state for MnT Operational Data
MnT Log Processor	Log processor for MnT service	Must be in Running state for MnT Operational Data
Certificate Authority Service	ISE Internal CA service	Must be in Running state if ISE internal CA is enabled

Required Internet URLs

The following table lists the features that make use of certain URLs. You must configure either your network firewall or a proxy server so that IP traffic can travel between Cisco ISE and these resources. If you cannot provide this access for any listed URL, the associated feature will be impaired or inoperable.

Table 23: Required URLs Access

Feature	URLs
Posture updates	https://www.cisco.com/ https://iseservice.cisco.com
Profiling Feed Service	https://ise.cisco.com
Smart Licensing	https://tools.cisco.com
Interactive Help	*.walkme.com *.walkmeusercontent.com

Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide

First Published: 2018-11-20

Last Modified: 2021-08-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

This preface describes this guide and provides information about the conventions used in this guide, along with details about related documentation. It includes the following sections:

Document Revision History

The following table shows the changes made to this document:

Date	Change Summary
November 2018	First version of the document.
July 2019	Added information on support for Google Cloud Platform (GCP).
February 2020	Added information on support for Microsoft Hyper-V.

Document Objectives

This publication describes the installation of the .

Audience

This publication is primarily designed for persons responsible for installing, maintaining, and troubleshooting the . The users of this guide should:

• Be familiar with electronic circuitry and wiring practices.

• Have experience working as electronic or electromechanical technicians.
• Have experience in installing high-end networking equipment.

Note Some procedures described in this guide require a certified electrician.

Conventions

Text Type	Indication
User input	Text the user should enter exactly as shown or keys a user should press appear in this font.
Document titles	Document titles appear in *this font*.
System output	Terminal sessions and information that the system displays appear in **this font**.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
String	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<>	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
! #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Tip Means *the following information will help you solve a problem.* The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means *reader be careful.* In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver: Means *the described action saves time.* You can save time by performing the action described in the paragraph.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS. Statement 1071

Related Documentation

See the following documentation for more information about the Cisco Catalyst 9800 Wireless Controller:

- *Release Notes for Cisco Catalyst 9800 Wireless Controller*
- *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*
- *Cisco Catalyst 9800 Series Wireless Controller Command Reference*
- *Cisco Wireless Solutions Software Compatibility Matrix*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

CHAPTER 1

Overview of Cisco Catalyst 9800 Wireless Controller for Cloud

Introduction

The Cisco Catalyst 9800-CL Cloud Wireless Controller (referred to as "controller" in this document) is a virtual wireless controller that is deployed on a Cisco Unified Computing System (UCS) server as a virtual machine (VM) instance on a Linux-based 64-bit guest operating system. This controller supports a subset of Cisco IOS XE software features and technologies, providing Cisco IOS XE features on a virtualization platform.

When the controller is deployed as a VM, the Cisco IOS XE software functions as if it were deployed on a traditional Cisco hardware platform.

Benefits of Virtualization

The controller uses the benefits of virtualization to provide the following:

- Hardware independence—Because the controller runs on a VM, it can be supported on the x86 hardware that the virtualization platform supports.
- Sharing of resources—The resources used by the controller are managed by the hypervisor; these resources can be shared among VMs. The amount of hardware resources that the VM server allocates to a specific VM can be reallocated to another VM on the server.
- Flexibility in deployment—You can easily move a VM from one server to another. Thus, you can move the controller from a server in one physical location to a server in another physical location without moving any hardware resources.

Software Configuration and Management

You can perform software configuration and management of the controller using the following methods:

- Use the virtual video graphics array (VGA) console or the console on the virtual serial port to access the Cisco IOS XE CLI commands.
- Use remote SSH or Telnet to access the Cisco IOS XE CLI commands.

Note The controller may reload when you run the **show redundancy trace main** command from the serial console.

Serial console is not recommended for large scale deployments. We recommend that you use Telnet or SSH for this purpose. For more information on how to add a virtual serial port, see *Adding Virtual Serial Port* in Cisco Catalyst C9800-CL Wireless Controller Virtual Deployment Guide.

Virtual Machines

The controller can run as a VM. A VM is a software implementation of a computing environment in which an operating system or program can be installed. The VM typically emulates a physical computing environment, but requests for CPU, memory, hard disk, network, and other hardware resources are managed by a virtualization layer that translates these requests to the underlying physical hardware.

You can deploy an Open Virtualization Archive (OVA) file for ESXi. The OVA file package simplifies the process of deploying a VM by providing a complete definition of the parameters and resource allocation requirements for the new VM.

An OVA file consists of a descriptor (.ovf) file, a storage (.vmdk) file, and a manifest (.mf) file.

- Descriptor or .ovf file—An XML file with .ovf as the extension, and consisting of all the metadata about the package. It encodes all the product details, virtual hardware requirements, and licensing.
- Storage or .vmdk file—A file format that encodes a single virtual disk from a VM.
- Manifest or .mf file—An optional file that stores the Secure Hash Algorithm (SHA) key generated during packaging.

Hypervisor Support

A hypervisor enables multiple operating systems to share a single hardware host machine. While each operating system appears to have the dedicated use of the host's processor, memory, and other resources, the hypervisor controls and allocates only the required resources to each operating system and ensures that the operating systems (VMs) do not disrupt each other.

Caution The controller might crash while taking a snapshot. We recommend that you use RAID0 configuration on the UCS to avoid a crash.

- Ensure that you use VMware ESXi Version 5.5 or later.

Supported Hypervisor Types

Installation of the controller is supported on selected Type 1 (native, bare metal) hypervisors. Installation is not supported on Type 2 (hosted) hypervisors, such as VMware Fusion, VMware Player, and Virtual Box.

Hypervisor vNIC Requirements

Depending on the controller's version number, each of the hypervisors support different virtual Network Interface Card (vNIC) types.

Table 1: vNIC Requirements for VMware ESXi

vNIC Requirements for VMware ESXi	Value
NIC Types Supported	VMXNET3
vNIC Hot Add Support	Yes
vNIC Hot Remove Support	Yes

Table 2: vNIC Requirements for Kernel-Based Virtual Machine (KVM)

vNIC Requirements for KVM	Value
NIC Types Supported	Virtio, ixgbevf, ixgbbe
vNIC Hot Add Support	Yes
vNIC Hot Remove Support	No

Table 3: vNIC Requirements for Amazon Web Services (AWS)

vNIC Requirements for AWS	Value
NIC Types Supported	VMXNET3
vNIC Hot Add Support	No
vNIC Hot Remove Support	No

Server Requirements

The server and processor requirements are different, depending on the software release. The following table captures the server requirements:

Table 4: Server Requirements

Software Release	Intel	AMD
Cisco IOS XE Gibraltar 16.10.1 and later	64-bit Intel Core2 and later-generation processors with virtualization technology extensions.	Equivalent of 64-bit Intel Core2 and later-generation processors with virtualization technology extensions.

Supported Templates and Hardware Requirements

From 17.3 release onwards, high throughput templates can be configured on the Cisco Catalyst 9800-CL Cloud Wireless Controller private cloud instances. With this enhancement, the throughput can be raised from 2 Gbps to 5 Gbps.

Table 5: Supported Templates and Hardware Requirements

Model Configuration	Small (Low Throughput)	Medium (Low Throughput)	Large (Low Throughput)	Small (High Throughput)	Medium (High Throughput)	Large (High Throughput)
Minimum number of vCPUs (Hyperthreading is not supported)	4	6	10	7	9	13
Minimum CPU Allocation (MHz)	4,000	6,000	10, 000	4000	6000	10,000
Minimum Memory (GB)	8	16	32	8	16	2
Required Storage (GB)	16	16	16	16	16	16
Virtual NICs (vNIC) (*) 3rd NIC for High Availability	2/(3)*	2/(3)*	2/(3)*	2/(3)*	2/(3)*	2/(3)*

Secure Boot

The secure boot feature prevents malicious software applications and unauthorized operating systems from loading into the controller during the controller startup process. If secure boot feature is enabled, only the authorized software applications boot up from the controller.

This feature ensures that the software applications that boot up on the controller are certified by Cisco. A secure compute system ensures that the intended software on the controller runs without malware or tampered software. The Unified Extensible Firmware Interface (UEFI) specification defines a secure boot methodology that prevents loading software that does not have an acceptable digital signature.

To view the secure boot mode and bootloader version, use the **show platform software system boot** command:

```
Device#show platform software system boot
Boot mode: UEFI or EFI Secure
Bootloader version: 1.1
```

Guidelines

- The following secure boot environments are supported:
  - ESXi version 6.5
  - KVM RHEL 7.5 using open stack license
  - NFVIS release 3.11
- Only EFI firmware modes support the secure boot feature.
- This feature is supported on VM created in Cisco IOS XE Bengaluru 17.6 release.
- GRUB3 and new disk partition layout is available from Cisco IOS XE Bengaluru 17.6 release.

Note VMs created prior to Cisco IOS XE Bengaluru 17.6 release support only BIOS mode.

Note If VM is installed using 17.6 ISO or OVA image, the downgrade to 17.3.4 fails during bootup with the following error message:

```
IOSXE image not compatible with installation,Failing boot..
```

Note Each hypervisor has a unique process to enable secure boot for the guest VMs. Refer to the relevant hypervisor documentation to enable secure boot. A set of high-level hypervisor specific steps to enable secure boot are mentioned below.

ESXi Secure Boot Setup

1. Create VM using ESXi version 6.5 or a later version using VM version 13.
2. To choose the EFI firmware mode, perform the following:
   a. Navigate to **Actions > Edit Settings**.
      The **Edit Settings** page is displayed.
   b. Navigate to **VM Options > Boot Options > Firmware**.
   c. From the **Choose which firmware should be used to boot the virtual machine** drop-down list, choose EFI option.
   d. Click Save.
3. Power up the VM to initialize the boot and wait for IOS prompt to complete.
4. Power down the VM.
5. To enable EFI secure boot, perform the following:
   a. Navigate to **Actions > Edit Settings**.
      The **Edit Settings** page is displayed.
   b. Navigate to **VM Options > Boot Options > Firmware**.
   c. Check the **Whether or not to enable UEFI secure boot for this VM** check box to enable EFI secure boot.
   d. Click Save.
6. Power up VM and the VNF boots up securely.

KVM Secure Boot Setup

1. Create a VM with a user-defined name.
2. Power down the VM after the VM is created and VNF IOS prompt is complete.
3. Install PK, KEK, and db certificates from the **EFI Firmware** menu and reset.
   To create the custom keys, see Custom Keys for Secure boot. For db certificates, see MicCorUEFCA2011_2011-06-27.crt and MicWinProPCA2011_2011-10-19.crt.
4. Secure boot the VM.

NFVIS Secure Boot Setup

1. Upgrade to NFVIS 3.11 release or a later one.
2. Register an ISRv EFI tarball with the NFVIS repository.
3. Create a VM using the registered EFI image.
4. Secure boot the VM.

Note Secure boot is disabled by default. To enable secure boot, you must change the firmware configurations from CIMC. Secure boot needs to boot from a separate UEFI partition.

To enable secure boot, perform the following:

a. Login to CIMC and use the **show bios detail** command to view the BIOS version.

```
ENCS# scope bios
ENCS/bios # show detail
BIOS:
    BIOS Version: " ENCS54_2.6 (Build Date: 07/12/2018)"
    Boot Order: EFI
    FW Updater/Recovery Status: Done, OK
    Active BIOS on next reboot: main
    UEFI Secure Boot: disabled
ENCS/bios #
```

b. Enable secure boot.

```
ENCS/bios # set secure-boot enable
Setting Value : enable
Commit Pending.
ENCS/bios *# commit
ENCS/bios # show detail
BIOS:
    BIOS Version: "ENCS54_2.6 (Build Date: 07/12/2018)"
    Boot Order: EFI
    FW Updater/Recovery Status: Done, OK
    Active BIOS on next reboot: main
    UEFI Secure Boot: enabled
ENCS/bios #
```

Note Legacy boot, UEFI boot, and UEFI secure boot are the three boot modes. Secure boot can only be used on a disk that has UEFI partition.

CHAPTER 2

Installing Controller in VMware Environment

Overview of VMware Environment

The controller runs on the Cisco IOS-XE operating system. The virtual installation images contain the underlying Cisco IOS-XE operating system and the Wireless Controller code. You must download the Cisco IOS XE software from Cisco.com and install it directly in the virtual machine (VM) environment. However, as part of the initial installation process, you must first provision the attributes of the VM so that the controller software can install and boot.

The high-level tasks required to install the controller are listed here.

Note The different installation options are dependent on the hypervisor being used.

Install the Controller Using an OVA File

1. Download the controller software (.ova file) from Cisco.com.
2. Create a network interface on the VM.
3. Deploy the OVA template using the VMware vSphere client to create a controller VM.
4. Power on the VM to boot the controller software.

Obtaining the Controller VM Image (OVA File)

1. Open the Cisco Catalyst 9800 Wireless Controller for Cloud product page.
2. Click the **Download Software** link to open the **Download Software** page.
3. In the **Download Software** page, select the model.
4. Click the corresponding Cisco IOS XE software. Note that the recommended Cisco IOS XE release is selected by default.
5. From the list of available images, click **Download Now** or **Add to Cart.**
6. Follow the instructions for downloading the software.

Installation Options

The controller currently supports only the following installation options:

- Deploying the OVA template in a VM environment.
- Deploying the controller using ISO installation.

Note The .ova file can be used only for first-time installation. It cannot be used for upgrading the Cisco IOS XE software version.

ROMMON and the Controller

The controller does not include a ROMMON image similar to what is included in many Cisco hardware-based devices. During the initial bootloader process, the installation script creates a clean version of the controller software image known as the Golden Image, and places it in a non-accessible partition. This clean version can be used if the software image is not working properly or cannot be booted.

Installing in a VMware ESXi Environment

This section includes information about VMware tools and VM requirements for the controller running the latest Cisco IOS XE software, as well as a list of the supported VM features.

The controller can run on the VMware ESXi hypervisor. You can use the same hypervisor to run several VMs.

The VMware vSphere web client is a web application that runs on the PC and accesses the vCenter Server. You can use the VMware vSphere Web Client software to create, configure, and manage VMs on the VMware vCenter Server and to start or stop the controller.

For more details about installing vSphere products, see the corresponding VMware product documentation.

Note Hot delete of the interface from the vSphere client is not supported until Cisco IOS XE Amsterdam 17.1.1s.

VMware Requirements

The VMware tools required to deploy the controller are as follows:

- VMware vSphere Web Client, The following version is supported:
  - VMware vSphere Web Client 6.0
- VMware vCenter Server.

  For the list of supported versions, see the Release Notes.
- VMware vSwitch. Standard or distributed vSwitches are supported.
- Hard drive. Only a single hard disk drive is supported. Multiple hard disk drives on a VM are not supported.
- vCPUs. The following vCPU configurations are supported:
  - Small Template—4 vCPUs (requires minimum 4-GB RAM allocation)
  - Medium Template—6 vCPUs (requires minimum 16-GB RAM allocation)
  - Large Template—10 vCPUs (requires minimum 32-GB RAM allocation)
- Virtual CPU core
- Virtual hard disk space—Minimum 8 GB is required.
- Virtual Network Interface Cards (vNICs).

Supported VMware Features and Operations

VMware supports various features and operations that allow you to manage your virtual applications and perform operations such as cloning, migration, shutdown, and resume.

Some of these operations cause the runtime state of the VM to be saved and then restored upon restarting. If the runtime state includes traffic-related state, on resumption or replay of the runtime state, additional errors, statistics, or messages are displayed on the user console. If the saved state is just configuration driven, you can use these features and operations without any issues.

Caution VMware functionalities, such as, vMotion, Snapshot, Distributed Resource Scheduler (DRS), vNIC Teaming and SR-IOV modes are supported. However, cloning from snapshots is not supported.

Also, vMotion, DRS, Snapshots, and vNIC Teaming are not supported when SR-IOV mode is enabled.

For more information, see the Cisco Catalyst 9800-CL Wireless Controller for Cloud Data Sheet.

For more information about VMware features and operations, see the corresponding VMware Documentation.

Creating a Network Interface on a VM

Perform the following tasks in the VMware vSphere Client to create a network interface.

Before you begin

This procedure is required only for the first installation of the controller.

Step 1 Log in to the VMware vSphere Client.
Step 2 In the vSphere GUI, click the **Configuration** tab.
Step 3 In the **Networking** area, click **Add Networking...**
Step 4 Under **Connection Type**, retain the default settings, and click **Next**.
Step 5 Under **Network Access**, select one of the VM names.
Step 6 Click **Next**.
Step 7 Under **Connection Settings**, enter a name in the **Network Label** field.
Step 8 From the **VLAN ID (Optional)** drop-down list, choose **All (4095)**.
Step 9 Click **Next**.
Step 10 Under **Summary**, confirm the updates and click **Finish**.

The newly added network interface is now available in the **Networking** area.

Configuring NIC Teaming on a Virtual Switch

You can include two or more physical NICs in a team to increase the network capacity of a virtual switch. This is termed as NIC teaming. To distribute how the virtual switch distributes the network traffic between the physical NICs in a team, you select load balancing depending on the needs and capabilities of your environment.

Perform the following tasks in the VMware vSphere Client to configure NIC teaming on a virtual switch.

Before you begin

This procedure is required only for configuring NIC teaming.

Note VMXNET3 is the virtual adapter type supported on the controller.

Step 1 Log in to the VMware vSphere Client.
Step 2 Navigate to the virtual switch.
Step 3 Click **Edit** to view the properties of the virtual switch.
Step 4 Navigate to **NIC Teaming** tab on the virtual switch properties page.
Step 5 From the **Load Balancing** drop-down menu, specify how the virtual switch load balances the outgoing traffic between the physical NICs in a team.

You can configure the following options on a virtual switch:

- Route based on the originating virtual port ID—Selects an uplink based on the virtual port IDs on the switch.
- Route based on IP hash—Selects an uplink based on a hash of the source and destination IP address of each packet.

- Route based on source MAC hash—Selects an uplink based on a hash of the source Ethernet.
- Use explicit failover order—Uses the highest order uplink from the list of active adapters that passes failover detection criteria. No actual load balancing is performed with this option.

Step 6 From the **Network Failover Detection** drop-down menu, specify a method for failover detection.

You can configure the following options on a virtual switch:

- Link Status Only—Relies on the link status provided by the network adapter. This option detects failures, such as, physical switch power failures and removed cables.
- Beacon Probing—Sends out and listens for beacon probes on all NICs in a team, and uses this details along with the link status to determine link failure.

Step 7 From the **Notify Switches** drop-down menu, select **Yes** or **No** to notify the switch for any failover.
Step 8 From the **Failback** drop-down menu, select whether a physical adapter is returned to active status after recovering from a failure.

If failback is set to **Yes**, the adapter is returned to active immediately after recovery. By default, a failback policy is enabled on a NIC team.

If failback is set to **No**, a failed adapter is left inactive after recovery until another active adapter fails and needs to be replaced.

Note If a physical NIC that stands first in the failover order experiences intermittent failures, the failback policy might lead to frequent updates in the NIC. The physical switch undergoes frequent changes in MAC addresses, and the physical port might not accept traffic immediately after an adapter becomes online. To minimize such delays, you can change the following settings on the physical switch:

- Disable Spanning Tree Protocol (STP) on physical NICs connected to the ESXi hosts.
- Enable PortFast mode or PortFast trunk mode for access and trunk interfaces respectively. This saves around 30 seconds during the initialization of the physical switch port.

Step 9 Review your settings and apply the configuration.

Information About Deploying Controller OVA on a VM using vSphere

You can use the controller OVA file package that is provided to deploy the controller on the VM.

The OVA can be deployed using the VMware vSphere Client, VMware OVF Tool, or the Common OVF Tool (COT).

Restrictions and Requirements

The following restrictions apply when deploying the OVA package on the VM:

- If the virtual CPU configuration is changed, the controller must be rebooted. Changing the RAM allocation does not require rebooting the controller.

- When deploying the OVA, the VM requires two virtual CD/DVD drives, one for the OVF environment file and another for the .iso file.

Deploying the Controller OVA File on a VM Using vSphere

Perform the following steps in the VMware vSphere Client:

You can use the controller OVA file package that is provided, to deploy the controller on the VM.

The OVA can be deployed using the VMware vSphere Client, VMware OVF Tool, or the Common OVF Tool.

Before you begin

- If the virtual CPU configuration is changed, the controller must be rebooted. However, changing the RAM allocation does not require rebooting the controller.
- When deploying the OVA, the VM requires two virtual CD/DVD drives, one for the OVF environment file and another for the .iso file.
- Ensure that the Network Interface is set up properly.

Step 1 Log in to the VMware vSphere Client.
Step 2 From the vSphere Client menu, choose **File > Deploy OVF Template**.
Step 3 In the **OVA** wizard, select the source of the controller OVA that is to be deployed.

The **OVF Template Details** window displays information about the OVA.

Step 4 Click **Next**.
Step 5 In the **Name and Location** field, specify the name for the VM and click **Next**.
Step 6 Click **Next**.
Step 7 Under **Deployment Configuration**, select the required profile from the drop-down list.
Step 8 Under **Disk Format**, retain the default settings (**Thick Provision Lazy Zeroed**) and click **Next**.
Step 9 From the **Network Mapping** drop-down list, allocate one or more virtual Network Interface Cards (vNICs) to the destination network. Connect each network to a unique interface. We recommend the following mapping:

- GigabitEthernet 1 to device management interface and map it to the out-of-band management network.
- GigabitEthernet 2 to wireless management interface and map it to the network to reach APs and services. Usually this interface is a trunk to carry multiple VLANs.
- GigabitEthernet 3 to high-availability interface and map it to a separate network for peer-to-peer communication for SSO.

Step 10 Under **Ready to Complete**, verify all the deployment settings.
Step 11 Click **Finish** to deploy the OVA.

The controller VM now appears on the left panel.

Step 12 Click **Power On** to automatically power on the VM.

Edit the Basic Properties of VM

Perform the following tasks in the VMware vSphere Client:

Step 1 Log in to the VMware vSphere Client.
Step 2 In the vSphere **GUI**, click the **Configuration** tab.
Step 3 In **Networking** area, click **Properties** of the newly added network interface.
Step 4 Click **Edit** to view the properties of the network interface..
Step 5 Click the **Security** tab.
Step 6 Uncheck the checked VM name.
Step 7 In the **Promiscuous Mode**, perform the following tasks:

The **Promiscuous Mode** is set to **Reject** by default.

Note Promiscuous mode is a security policy which can be defined at the virtual switch or port-group level in vSphere ESXi. Tagged traffic will not flow properly without this mode.

- Check the check box.
- From the drop-down list, select **Accept** to view the traffic sent and received through this switch.

Note Ensure that **Forged Transmits** is also set to **Accept**.

Step 8 Click **OK**, and then click **Close**.

Configuring SR-IOV for VMware ESXi

Recommended Software Versions for SR-IOV

Table 5: List of Supported NIC Types

NIC	Firmware	Driver Version	Host OS
Intel x710	7.10	i40en 1.10.6 INETCLI Plugin version 1.4.1	VMware Version 6.5 and above

Configuring SR-IOV Mode on the Interface

Step 1 Create a port group without any ports.
Step 2 Create a dummy virtual switch and attach the port group created in **Step 1** to this switch.

Step 3 Enable SR-IOV for x710 PCI device ports from **Host > Manage > Hardware**.

Note One VF is created on each port to maximize performance.

Step 4 Create an eWLC instance. While adding the network adapter, perform the following:

a. Choose **Network Adapter** as the created port group.
b. Choose **Adapter Type** as the SR-IOV passthrough.
c. Choose **Physical Function** as the one mapped to the port on which the SR-IOV is enabled.
d. Set the **Guest OS MTU Change** to **Allow**.
e. Click **Save**.

Enabling Trusted Mode and Disabling Spoof Check

To enable SSH to ESXi from the GUI, perform the following:

Step 1 Navigate to **Host > Actions > Services > Enable SSH**.
Step 2 Set SSH to **ESXi**.

To disable spoof check, perform the following:

While the controller is booting up, set the trusted mode and spoof check using the following command:

esxcli intnet srievnic vf set -t on -s off -v *<vf-id>* **-n** *<physical_port_name>*

Here,

<physical_port_name> is the SR-IOV port to which the VM is associated.

<vf-id> is the VF ID assigned to the VM instance.

Sample output:

```
[root@localhost:~] esxcli intnet srievnic vf set -t on -s off -v 0 -n vmnic6
```

Note To verify if the VF ID has been assigned to the controller, check the **vmkernel.log** file in /var/log location.

Configuring SR-IOV Setting Persistence

SR-IOV configurations configured in the above way are not persistent across reboots. To resolve this issue, you can execute the above configuration as a service that is auto-enabled on host reboots.

Step 1 For firmware and driver versions prior to and including firmware version 7.0, and driver version 1.8.6, you need to stop the VM load at boot up and perform *Enabling Trusted Mode and Disabling Spoof Check*.
Step 2 For firmware and driver versions above and including firmware version 7.10, and driver version 1.10.6, enter the following commands once after setting the trusted mode and spoof check to make the setting permanent:

esxcli system module parameters set -p max_vfs=1,1,1,1 -m i40en
esxcli system module parameters set -m i40en -p trust_all_vfs=1,1,1,1

...ying SR-IOV Driver and Firmware Version

You can verify the NICs using the following command:

esxcli network nic list

```
[root@localhost:~] esxcli network nic list

Name    PCI Device    Driver  Admin Status  Link Status  Speed  Duplex  MAC Address
   MTU  Description

------  ------------  ------  ------------  -----------  -----  ------  -----------------
  ----  -----------------------------------------------------

vmnic0  0000:87:00.0  i40en   Up            Up           10000  Full    3c:fd:fe:ec:c9:f8
  1500  Intel Corporation Ethernet Controller X710 for 10GbE SFP+

vmnic1  0000:87:00.1  i40en   Up            Down             0  Half    3c:fd:fe:ec:c9:f9
  1500  Intel Corporation Ethernet Controller X710
```

You can view the parameters for a particular interface using the following command:

esxcli network nic get -n vmnic6

```
[root@localhost:~] esxcli network nic get -n vmnic6
Advertised Auto Negotiation: true

   Advertised Link Modes: Auto, 10000baseSR/Full, 10000baseSR/Full

   Auto Negotiation: true

   Cable Type: FIBRE

   Current Message Level: 0

   Driver Info:

         Bus Info: 0000:87:00:0

         Driver: i40en

         Firmware Version: 7.10 0x80006471 1.2527.0

         Version: 1.12.6
[root@localhost:~] esxcli intnet srievnic vf get -n vmnic6
VF ID          Trusted        Spoof Check
-----          -------        -----------
0              true           false
```

You can verify the processor, memory, vNIC, hypervisor, and throughput profile details using the following command:

```
Device# show platform software system all
```



```
Device# show platform software system all

Controller Details:
-------------------
VM Template: medium
Throughput Profile: high
AP Scale: 3000
Client Scale: 32000
MACSEC instances: 0
Processor Details
-----------------
Number of Processors : 6
Processor id : 0 - 5
Vendor id : GenuineIntel
cpu MHz   : 2593.748
cache size : 4096 KB
Crypto Supported : Yes
Model name : Intel Core Processor (Haswell, IBRS)
Memory Details
--------------
Physical Memory : 56363364KB

VNIC Details
------------
Name            Mac Address       Driver Name      Status  Platform MTU
GigabitEthernet1  3c:fd:fe:ec:ccc0  net_i40e_vf      DOWN    1522
GigabitEthernet2  3c:fd:fe:ec:cdd0  net_i40e_vf      DOWN    1522

Hypervisor Details
------------------
Hypervisor: VMWARE
Manufacturer: VMware, Inc.
Product Name: VMware Virtual Platform
Serial Number: VMware-42 00 f0 d7 62 5e 5b 5a-7b 6e ac 81 5d de ac 71
UUID: 0E354A9D-DE5E-470D-9B5D-B252155193DB
Image_Variant :

Boot Details
------------
Boot mode: BIOS
Bootloader Version: 1.1
```

For information on the firmware for Intel NIC, see:

https://downloadcenter.intel.com/product/82947/Intel-Ethernet-Controller-X710-Series

For information on the driver for Intel and Cisco NIC, see:

https://www.vmware.com/resources/compatibility/detail.php%3FdeviceCategory%3Dio%25productid%3D37998

For information on the firmware for Cisco NIC, see:

https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/tsd-products-support-series-home.html

Creating a VM for Controller Using an ISO Image

The following procedure provides general guidelines about how to deploy the controller using VMware vSphere. However, the exact steps that you should perform may vary, depending on the characteristics of your VMware environment and setup.

Step 1 Start virt-manager **Applications > System Tools > Virtual Machine Manager.**
You may be asked to select the hypervisor and/or enter your root password.

Step 2 Select **File** option on top and click **New Virtual Machine** option.

Step 3 Enter the virtual machine details:
a) Specify a **Name.**
b) For the operating system, select **Import existing disk image.**
This method allows you to import a disk image (containing a pre-installed, bootable operating system, if you select the qcow2 image) to it.
c) Click **Forward** to continue.

Step 4 Select the controller qcow2 image path.

Step 5 Configure the memory and CPU options:
a) Set **Memory** (RAM) to *8192*.
b) Set **CPUs** to *4*.
c) Click **Forward** to continue.

Step 6 Enter the instance name.

Step 7 Check the **Customize configuration before install** box first before you click **Finish.**
This allows you to add more NICs.

Step 8 Select the **Network.**
Choose either bridge or network.

Step 9 Click **Finish.**

Step 10 Double click on the **Instance name** to edit it.

Step 11 Select *to* get the Instance information

Step 12 Select **Begin Installation** to start the Instance.

Step 13 Click the **Monitor** symbol to go to the Virtual Console.

Configuring SR-IOV for KVM

Recommended Software Versions for SR-IOV

Table 3: List of Supported NIC Types

NIC	Firmware	Driver Version	Host OS
Intel x710	7.10	I40e 2.10.19.82	KVM RedHat Version 7.5 and above

NIC	Firmware	Driver Version	Host OS
Cisco/ized x710	7.0	I40e 2.10.19.82	KVM RedHat Version 7.5 and above

Enabling Intel VT-D

Note You need to have root permissions to perform subsequent tasks.

To enable Intel VT-D, perform the following steps:

Step 1 In the **/etc/sysconfig/grub** file and **GRUB_CMDLINX_LINUX** line, add the **intel_iommu=on** and **iommu=pt** parameters at the end.

Step 2 Regenerate the **/etc/grub2.cfg** file by executing the following command:
grub2-mkconfig -o /etc/grub2.cfg
Note In case of EFI, execute the following command:
grub2-mkconfig -o /etc/grub2-efi.cfg

Step 3 Reboot the system for the changes to take effect.
Your system is now capable of PCI device assignment.

Configuring SR-IOV Mode Virtual Functions (VFs) on the Interface

If VF is not available, configure SR-IOV VF using the following commands:

Step 1 Configure VF on the interface:
echo "no_of_vfs" > /sys/class/net/<interface_name>/device/sriov_numvfs
Sample output:

```
echo 1 > /sys/class/net/enp129s0f0/device/sriov_numvfs
```

Here, one VF is created for each port for maximum performance.

Step 2 Configure spoofchack, trust mode, and MAC on the VF using the following commands:

```
ip link set dev enp129s0f0 vf 0 trust on
ip link set enp129s0f0 vf 0 spoofchk off
ip link set enp129s0f0 vf 0 mac 3c:fd:fe:de:ec:bc
```

Note The MAC addresses must be unique.

Step 3 Verify the settings using the following command:
ip link show *interface_name*
Sample output:

```
ip link show enp129s0f0
6: enp129s0f0: <BROADCAST,MULTICAST> mtu 1500 qdisc mqprio state DOWN mode DEFAULT group default qlen
 1000
link/ether 3c:fd:fe:de:ec:bc brd ff:ff:ff:ff:ff:ff
vf 0 MAC 3c:fd:fe:de:ec:bc, spoof checking off, link-state auto, trust on
```

Configuring SR-IOV Setting Persistence

SR-IOV configurations configured in the above way are not persistent across reboots. To resolve this issue, you can execute the above configuration as a service that is auto-enabled on host reboots.

Step 1 Create a bash script with the commands to be persisted. You need to write the script in **/usr/bin/sriov-config** file as follows:

```
#!/bin/sh
echo "no_of_vfs" > /sys/class/net/<interface_name>/device/sriov_numvfs
ip link set dev <interface_name> vf 0 trust on
ip link set <interface name> vf 0 spoofchk off
ip link set <interface_name> vf 0 mac 3c:fd:fe:de:ec:bc
```

Sample output:

```
#!/bin/sh
echo 1 > /sys/class/net/enp129s0f0/device/sriov_numvfs
ip link set dev enp129s0f0 vf 0 trust on
ip link set enp129s0f0 vf 0 spoofchk off
ip link set enp129s0f0 vf 0 mac 3c:fd:fe:de:ec:bc
```

Note You need to repeat the same steps for all VFs.

Step 2 Provide execute permission for the script:
chmod 777 /usr/bin/sriov-config

Step 3 Create the system service: Define a new system service to be executed at the end of the boot. This service executes the bash script which has the required sriov commands as mentioned in **Step 1.**
Note Create a new file named **sriov.service** in **/usr/lib/systemd/system** and add the following content:

```
[Unit]
Description=SR-IOV Configuration
After=rc-local.service
Before=getty.target
[Service]
Type=oneshot
ExecStart=/usr/bin/sriov-config
[Install]
WantedBy=multi-user.target
```


Note The **ExecStart=/usr/bin/sriov-config** command line executes the script.

Step 4 Enable and start the **sriov.service** using the following command:
systemctl --now enable sriov.service
Note This command starts the service immediately and ensures that the service is run every time the ho s.

For more information on the SR-IOV configuration for KVM, see:
https://www.intel.com/content/www/us/en/embedded/products/networking/xl710-sr-iov-config-guide-gbe-linux-brief.html

Attaching the SR-IOV to the Controller

Attaching to a New Virtual Machine Using Command Line

Use the **host device** option of **virt-install** to add the PCI VF devices. Use the information from **Step 1** [Configuring SR-IOV Mode Virtual Functions (VFs) on the Interface, on page 28] and PCI BDF number to attach the devices.

Virtual Functions on Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (enp129s0f0):

```
PCI BDF                                    Interface
=======                                    =========
0000:81:09.0                 enp129s0f0
0000:81:09.1                               enp129s0f1
```

Creating and Launching a VM

To create and launch a VM, use the following command:

```
sudo virt-install --virt-type=kvm --name sriov_sriov_3-14 --ram 16384 --vcpus=8 --boo
--cdrom=/home/C9800-CL-universalk9.BLD_POLARIS_DEV_LATEST_2020031e_052619-serial.iso --network
 none --host-device=pci_0000_14_06_0 --host-device=pci_0000_14_06_1 --graphics vnc --dis
path=/var/lib/libvirt/images/sriov_sriov_3-14.qcow2,size=8,bus=virtio,format=qcow2
```

You get to view the VM console using the following command:

```
virsh console sriov_sriov_3-14
Connected to domain sriov_sriov_3-14
Escape character is ^]
```

You can enter the following command to verify the SR-IOV drivers for the interface:

Device > enable

Device #show platform software vnic-if interface-mapping

```
Device # show platform software vnic-if interface-mapping
------------------------------------------------------------
Interface Name      Driver Name      Mac Addr
------------------------------------------------------------
GigabitEthernet2    net_i40e_vf      3c:fd:fe:de:ec:bd
GigabitEthernet3    net_i40e_vf      3c:fd:fe:de:ec:be
------------------------------------------------------------
```

Note The MAC address mentioned above is the same as the one that is set for the VF.

You can verify the processor, memory, vNIC, hypervisor, and throughput profile details using the following command:

Device # show platform software system all

```
Device# show platform software system all
Controller Details:
=================
VM Template: medium
Throughput Profile: high
AP Scale: 3000
Client Scale: 32000
WNCD instances: 3

Processor Details
=================
Number of Processors : 9
Processor : 1 - 9
vendor_id : GenuineIntel
cpu MHz  : 2593.749
cache size : 4096 KB
Crypto Supported : Yes
model name : Intel Core Processor (Haswell, IBRS)
Memory Details
==============
Physical Memory : 16363364KB

VNIC Details
============
Name                Mac Address    Driver Name    Status  Platform MTU
GigabitEthernet1    3cfd.fede.cdbc  net_i40e_vf    DOWN    1522
GigabitEthernet2    3cfd.fede.cdbd  net_i40e_vf    DOWN    1522

Hypervisor Details
==================
Hypervisor: KVM
Manufacturer: Red Hat
Product Name: KVM
Serial Number: Not Specified
UUID: 0E354EDD-DE6E-405D-9B3D-0252155190B9
image_variant :

Boot Details
==================
Boot mode: BIOS
Bootloader version: 1.1
```

Attaching an Interface to the Controller Using KVM VMM (virt-manager)

In the virt-manager, select **Hardware > Add Hardware** to add the PCI host device to the VM. Navigate to the NIC card and choose the VF that needs to be attached to the VM.

Once the **PCI** is added to the VM, you can start the VM.

57

Verifying SR-IOV Driver and Firmware Version

You can verify the ethernet and driver versions using the following command:

`ethtool -i <interface_name>`

Note You need to execute this command on the host machine.

```
[root@cpp-rhel-perf ~]# ethtool -i enp129s0f0
driver: i40e
version: 2.10.19.82
firmware-version: 7.10 0x80006456 1.2527.0
expansion-rom-version:
bus-info: 0000:81:00.0
```

You can print the ethernet information, driver versions, and SR-IOV VF names using the following command:

`lspci | grep -i eth`

```
[root@cpp-rhel-perf ~]# lspci | grep -i eth
81:00.0 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev
 02)
81:00.1 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev
 02)
81:02.0 Ethernet controller: Intel Corporation Ethernet Virtual Function 700 Series (rev
02)
81:0a.0 Ethernet controller: Intel Corporation Ethernet Virtual Function 700 Series (rev
02)
```

For information on the firmware for Intel NIC, see:

https://downloadcenter.intel.com/product/82947/Intel-Ethernet-Controller-X710-Series

For information on the driver for Intel and Cisco NIC, see:

https://downloadcenter.intel.com/download/24411/Intel-Network-Adapter-Driver-for-PCIe-40-Gigabit-Ethernet-Network-Connections-Under-Linux-?product=82947

For information on the firmware for Cisco NIC, see:

https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/tsd-products-support-series-home.html

CHAPTER 4

Installing the Controller in NFVIS Environment

Overview of Cisco Enterprise Network Function Virtualization Infrastructure Software

Cisco Enterprise Network Function Virtualization Infrastructure Software (Cisco Enterprise NFVIS) is a Linux-based infrastructure software designed to help service providers and enterprises dynamically deploy virtualized network functions, such as a virtual router, firewall, and WAN acceleration, on a supported Cisco device. Addition of a physical device for every network function is not required; you can use automated provisioning and centralized management.

Cisco Enterprise NFVIS solution helps you convert your critical network functions into software, making it possible to deploy network services in minutes across dispersed locations. It provides a fully integrated platform that can run on top of a diverse network of both virtual and physical devices.

The Cisco 5400 Series Enterprise Network Compute System combines routing, switching, storage, processing, and a host of other computing and networking activities into a compact 1-RU box. This high-performance unit achieves this goal by providing the infrastructure to deploy virtualized network functions and acting as a server that addresses processing, workload, and storage challenges.

Installation Procedure

VM lifecycle management refers to the entire process of registering, deploying, updating, monitoring VMs, and getting them service chained as per your requirements. You can perform these tasks using the Cisco Enterprise NFVIS portal.

Register a VM Image

To register a VM image, you must first copy or download the relevant VM image to the NFVIS server, or host the image on a HTTP or HTTPs server. After you download the file, you can register the image using the

registration API. This API allows you to specify the file path to the location (on an HTTP or HTTPs server) where the tar.gz file is hosted. Registering the image is a one-time activity. After an image is registered on the HTTP or HTTPs server, and is in active state, you can perform multiple VM deployments using the registered image.

Customizing the Setup

After registering a VM image, you can optionally create a custom profile or flavor for the VM image if the profiles defined in the image file do not match your requirement. The flavor creation option lets you provide specific profiling details for a VM image, such as the virtual CPU on which the VM will run, and the amount of virtual memory the VM will consume.

Depending on the topology requirement, you can create additional networks and bridges to attach the VM to during deployment.

Deploying a VM

A VM can be deployed using the deployment API. This API allows you to provide values to the parameters that are passed to the system during deployment. Depending on the VM you are deploying, some parameters are mandatory and others optional.

Managing and Monitoring a VM

You can monitor a VM using APIs and commands that enable you to get the VM status and debug logs. Using VM management APIs, you can start, stop, or reboot a VM, and view the statistics for a VM, such as CPU usage.

A VM can also be managed by changing or updating its profile. You can change a VM's profile to one of the existing profiles in the image file; alternatively, you can create a new custom profile for the VM. The vNICs on a VM can also be added or updated.

Uploading Image on NFVIS

Follow the procedure given below to upload an image to NFVIS:

Step 1 Select **VM Life Cycle > Image Repository**.

Step 2 Select the **Image Registration** tab and click upload arrow next to **Images**.

Step 3 Select the file from **Drop Files** or **Click** option.

Step 4 Click **Start** to upload the image.

After the image is uploaded, NFVIS creates respective profiles and registers the image. You can find your file listed under the Images section on the same page.

Creating a VM Package Using Web Interface

Follow the procedure given below to create VM image using web interface:

Step 1 From ENCS, select **Image Packaging** tab and click on the create icon next to **VM Packages**.
Step 2 Enter the details in **Image Packaging** tab.
Step 3 Click **Submit**.
The bootstrap files are uploaded.
After the image is created, you have to register it so that the profiles are properly populated in the ENCS.
Step 4 Select the image you created and click on **Register**.

Creating a Network

Follow the procedure given below to create a network:

Step 1 From ENCS, select **VM Life Cycle> Networking** .
This opens up Networks & Bridges window.
Step 2 Click on the create icon next to **Networks & Bridges**.
Step 3 Enter values for **Network**, **Mode**, **Vlan**, **Bridge** and **Interface**.
Note Single Root Input/Output Virtualization (SRIOV) is not supported.
Step 5 Click **Submit**.
This creates the network.

Deploying the Controller on NFVIS

Follow the procedure given below to deploy the controller on NFVIS:

Step 1 From ENCS, select **VM Life Cycle > Deploy**.
This opens up the VM Deployment window.
Step 2 From the VM Deployment window, drag and drop the controller icon to the pane below and map to the desired networks as required.
Note We support only 1000 APs and 10000 clients.
Step 3 In **VM Details** area, enter the **VM Name**.
Step 4 Select the **Image** name from the drop-down.
Step 5 Select the Profile name from the drop-down.

Step 6 Select the **Bootstrap Config** option for providing the bootstrap configuration file before deploying the VM.
Ensure that you use the filename "iosxe_config.txt" for the bootstrap configuration file.
Step 7 Click **Deploy**.

What to do next

After deploying the VM instance, you can check the instance details in **Manage** tab, which lists the summary of VM instances.
You can click the **Console** symbol next to the VM to get the console access.

Viewing VM Resource Allocation

Follow the procedure given below to view the VM resource allocations:

Step 1 From ENCS, select **VM Life Cycle> Resource Allocation**.
This opens up the VM CPU Allocation tab, which displays the overall CPU allocations.
Step 2 Click **VM Memory Allocation** tab.
This tab shows the overall memory allocations.
Step 3 Click **VM Disk Allocation** tab.
This tab shows the overall disk allocations.

Viewing VM Statistics

Follow the procedure given below to view the VM resource utilization:

Step 1 From ENCS, select **VM Life Cycle> VM Monitoring**.
This opens up the VM CPU Utilization tab, which displays the overall CPU utilization per VM.
Step 2 Click **Memory Allocation** tab.
This tab displays the memory utilization per VM.
Step 3 Click **VNIC Utilization** tab.
This tab displays the VNIC utilization per VM.
Step 4 Click **Disk Utilization** tab.

This tab displays the disk utilization per VM.

CHAPTER 5

Installing the Controller in AWS Environment

Overview on Amazon Web Services

The controller can be deployed on Amazon Web Services (AWS) for public cloud solutions.

Prerequisites

Before attempting to launch the controller on AWS, the following prerequisites should be met:

- Create an AWS account.
- Install an SSH client (for example, Putty on Windows or Terminal on Macintosh) to access the controller console.
- Determine the instance type that you want to deploy.
- Create an IAM user.
- Create a key pair.
- Create a VPC.
- Create a security group.
- Create a VPN gateway.
- Create subnets.
- For each remote site, create:
  - Create a customer gateway

- Create a VPN connection.

General Information

- All interfaces in the public cloud are Layer 3 and there are no trunk interfaces.
- All the public cloud IP allocations are done using DHCP on public cloud. You can decide on the IP to be assigned to the controller.
- Supports only one interface, which is shared by device management and wireless management.

Creating a Virtual Private Cloud

Follow the procedure given below to configure a VPC in AWS:

Before you begin

- A VPC is a virtual network dedicated to your AWS account and logically isolated from other virtual networks in the AWS Cloud.
- You can specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.
- You can optionally connect your VPC to your own corporate data center using an IPsec AWS-managed VPN connection, making the AWS Cloud an extension of your data center.

Note A VPN connection consists of a virtual private gateway attached to your VPC and a customer gateway located in your data center. A virtual private gateway is the VPN concentrator on the Amazon side of the VPN connection. A customer gateway is a physical device or software appliance on your side of the VPN connection.

Step 1 Select a VPC configuration, using the navigation path: **AWS Console>VPC Dashboard> Launch VPC Wizard> VPC with a Private Subnet Only and Hardware VPN Access**.

Step 2 Enter details at the **VPC with a Private Subnet Only and Hardware VPN Access** window.

Step 3 Create a subnet, using the navigation path: **VPC Console> Subnets> Create Subnet**

Step 4 Create a security group, using the navigation path: **VPC Console> Security Groups> Create Security Group**

A security group is a virtual firewall that controls traffic to and from one or more instances. When an instance is brought up, you can associate one or more security groups with it. You can use the default security group for the instances, but we recommend that you create a security group that reflects the role of your instances.

Step 5 Click **Create**.

This creates a VPC.

Creating a Virtual Private Gateway

Follow the procedure given below to create an AWS Virtual Private Gateway:

Before you begin

Step 1 Click **VPN Connections> Virtual Private Gateway**.

The Create Virtual Private Gateway window is displayed. Enter the following details:

a) Enter a Name Tag.

Use the AWS VPN router name.

b) Choose an ASN.

You can either use a custom ASN or use the default one selected by amazon gateway.

Note After creating the AWS VPN gateway, it will be shown as detached and you need to attach it to a VPC.

Step 2 Click on **Actions** button, choose **Attach to VPC**.

Step 3 From the pop-up window, select the VPC created earlier.

Attaches the AWS VPN to the VPC.

Creating a Customer Gateway

Follow the procedure given below to create a customer gateway:

Step 1 From the AWS console, go to the **VPC** dashboard.

Step 2 Click **VPN Connections> Customer Gateways.**

Step 3 Click **Create Customer Gateway.**

The Create Customer Gateway window is displayed. Enter the following details:

a) Name of your VPN router.
b) Select routing as *dynamic* or *static*.
c) Enter the external, internet routable address of your router or firewall.

Step 4 Click **Create Customer Gateway.**

Creating a VPN Connection

Follow the procedure given below to create a customer gateway:

Step 1 From the AWS console, go to the **VPC** dashboard.

Step 2 Click **VPN Connections> VPN Connections.**

Step 3 Click **Create VPN Connection.**

The Create VPN Connection window is displayed. Enter the following details:

a) Name of the VPN connection.
b) Select the AWS VPN gateway and customer gateway.
c) Select routing as *dynamic* or *static*.
d) Enter the remote subnets reachable through VPN.

The remote subnets are the remote network where your APs will be on-prem.

Step 4 (Optional) Assign subnet and keys for tunnel interfaces for IPSEC VPN.

AWS creates 2 tunnel interfaces for redundancy. If you do not specify details, AWS randomly generates tunnel options.

Step 5 Click **Create VPN Connection.**

This creates a VPN connection. It takes a few minutes to set up the connection and change the status from *pending* to *available*.

Step 6 While the VPN is being created, you can download the configuration to deploy in the customer VPN router. Click **Download Configuration.**

Step 7 From the pop-up window, select the brand and type of customer VPN router.

Step 8 Click **Download.**

Creating a Key Pair

Follow the procedure given below to create a customer gateway:

Step 1 From the AWS console, go to the **EC2** dashboard.

Step 2 Click **Network & Security > Key pairs** .

Step 3 Click **Create Key Pair.**

Installing the Controller on AWS Using Cloud Formation Template

Before you begin

- A VPC is created with the desired subnet for the controller management interface.
- A managed VPN connection is created from the Enterprise site or sites to the VPC.

- Download the CloudFormation template from AWS marketplace and save it on your computer.

Step 1 From the AWS console, go to the **CloudFormation** page.
Step 2 Click **Create Stack**.
Step 3 From **Choose a template** section, select upload template to Amazon S3 option.

This loads the *json* file directly to AWS.

Step 4 Click **Next**.

This opens the **Specify Details** page.

Step 5 Enter the **Stack** and **Instance Details**.

Enter any name for the stack you want. Hostname is the controller name. Instance Key Pair is the name of the keypair. AMI id is the AMI for the EC2 instance.

Step 6 Click **Next**.

This opens the **Network Details** page.

Step 7 Enter **Network** and **User** details.

For the Management Network and Management Security, use the drop-downs to select subnet and security group. Enter an username and password to connect to the instance remotely.

Step 8 Click **Next**.

Wait for the status to go from 'CREATE_IN_PROGRESS' to 'CREATE_COMPLETE'.

Step 9 Select the **Instance Type**.
Step 10 Go to **EC2** dashboard, click **Running Instances**.

The new instance will be in Status Checks (System Status Checks & Instance Status Checks) initializing. Wait for few minutes until it turns green.

When the status turns green, your controller in the cloud is ready to use. You can connect using SSH using the defined credentials or using the .pem file.

Installing the Controller Using AWS Console

Follow the procedure given below to install controller with AWS console:

Step 1 From the AWS console, go to the **EC2 Management** page.
Step 2 Click **Launch Instance**.
Step 3 Click **My AMIs** to select the Cisco Catalyst 9800 Wireless Controller for Cloud AMI.
Step 4 Choose an **Instance Type**.

We recommended that you choose the instances as per your requirements.

Step 5 Configure **Instance Details**.
a) Choose **Availability Zone**.
b) Choose **Network**.
c) Select **Subnet**.
d) Associate an IAM role to restrict or allow usage of instance to other users.

Note You must disable public IP during bring-up.

Step 6 Go to **Add Storage** page.

You can use this optional step to specify additional volumes to be attached to the instance.

Step 7 Go to **Add Tags** page.
a) Enter **Tag Volumes**.
b) Select **Interfaces**.
c) Select **Instance**.

Step 8 Go to **Configure Security Group**. Choose a security group. If a relevant one does not exist, create a new one.
Step 9 Click **Review and Launch**. Review the configuration of your instance.
Step 10 Click **Launch Instances**.

Before launching your instance, you need a key pair to access the instance. Key pair consists of a public key that AWS stores and a private key that you store. If you do not have a key, click **Create a new keypair**, and create a new one, else choose an existing keypair.

What to do next

After the instance is up, you can connect to the Cisco Catalyst 9800 Wireless Controller for Cloud instance using the following unix command on your terminal:

```
ssh -i <ssh_key_pair_file> <username>@<public-ip(DNS name)>
```

You can obtain the IP and the DNS name from the description of the instance on the EC2 instance console.

Bootstrap Properties for AWS

Table 3: Bootstrap Properties for AWS

Property	Description
hostname	Configures the hostname of the router, as shown in the following example: `hostname <C9800-CL-hostname>`
domain-name	Configures the network domain name, as shown in the following example: `domain-name <cisco.com>`

Property	Description
mgmt-ipv4-gateway	Configures the IPv4 management default gateway address, as shown in the following example: `mgmt-ipv4-gateway <ip>`

ios-config	Enables execution of a Cisco IOS command. To execute multiple commands, use multiple instances of ios-config, with a number appended to each instance, for example, ios-config-1, ios-config-2, and so on.
	When you specify a Cisco IOS command, use escape characters to pass special characters that are within the command: ampersand(&), double quotes("), single quotes('), less than(<) or greater than(>). See "ios-config-5" in the following example:
	`ios-config-1="username cisco priv 15 pass cisco123"`
	`ios-config-2="ip ssh source-interface GigabitEthernet1"`
	`ios-config-3="ip domain-name cisco.com"`
	`ios-config-4="snmp-server enable traps"`
	`ios-config-5="interface GigabitEthernet1 \n ip address dhcp \n no shut"`

CHAPTER 6

Installing Controller on GCP

Installing Cisco Catalyst 9800 Wireless Controller for Cloud on GCP

The Cisco Catalyst 9800 Wireless Controller for Cloud is a virtual controller running Cisco IOS XE. Most of the Cisco IOS XE features are available on the cloud controller and you can choose to deploy the controller software on Google Cloud Platform (GCP).

To deploy a Cisco Catalyst 9800 Wireless Controller for Cloud on GCP, you must create a project with the following resources: virtual machines, interfaces, virtual private cloud (VPC) networks, routes, public IP addresses, firewall rules, and storage. Resources that exist in different projects can only connect through an external network.

Google Compute Engine instances can run the public images for Linux and Windows Server that Google provides as well as private custom images that you can create or import from your existing systems. Compute instances use SSH public-key authentication. Certain Compute Engine resources live in regions or zones. Resources that live in a zone, such as instances or persistent disks, are referred to as zonal resources.

Other resources, like static external IP addresses, are regional. Regional resources can be used by any resources in that region, regardless of zone, while zonal resources can only be used by other resources in the same zone. A firewall enables you to specify the protocols, ports, and source IP ranges that can reach your instances using security groups. Static IPv4 addresses are used for dynamic cloud computing. Metadata, also known as tags, allows you to create and assign your GCP compute resources.

GPC VPC Concepts

- A VPC network, sometimes just called a *network*, is a virtual version of a physical network, like a data center network.
- You can launch your GCP cloud resources, such as GCP compute instances, into your VPC.

- You can specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.
- You can optionally connect your VPC to your own corporate data center using an IPsec GCP managed VPN connection, making the GCP Cloud an extension of your data center.

Creating a VPC in GCP

Follow the procedure given below to configure a VPC network in GCP:

Step 1 From the navigation menu in the GCP console, scroll down to **VPC network** and select **VPC networks.**

Step 2 Click **CREATE VPC NETWORK.**

Step 3 Enter a **Name** for the network.

For example, use *custom-network1*.

Step 4 Enter a **Description** for the network.

Step 5 In the **Subnets** section, click **Add Subnet.**

The New subnet dialog box opens. Enter a name for the subnet, for example *subnet-europe-west-192.*

Step 6 Select a **Region.**

For example, use *europe-west1.*

Step 7 Enter an **IP address range.**

For example, use *192.168.5.0/24.*

Step 8 Click **Done.**

This creates a subnet.

Perform Step 5 to Step 9 to create a subnet for the VPC network. You can add multiple subnets to the network.

Step 9 Click **Create.**

This creates a VPC network.

Creating a VPN Connection Using Dynamic Routing

Follow the procedure given below to create a customer gateway:

Step 1 From the GCP console, go to the **VPN** page.

Step 2 Click **Create VPN Connection.**

The Create VPN Connection window is displayed. Enter the following details:

a) Name of the **VPN** gateway.

b) Select the **VPC** network.

The network containing the instances the VPN gateway is going to serve.

c) Select the **Region.**

The region to locate the VPN gateway. Normally, this is the region that contains the instances you wish to reach.

d) Enter the **IP address.**

Select a pre-existing static external IP address. If you don't have a static external IP address, create one by clicking New static IP address from the drop-down menu.

e) Enter the **Peer IP address.**

Public IP address of the peer gateway.

f) Enter **IKE** version.

IKEv2 is preferred, but IKEv1 is supported if that is all the peer gateway can manage.

g) Enter the **Shared Secret.**

Character string used in establishing encryption for that tunnel. You must enter the same shared secret into both VPN gateways. If the VPN gateway device on the peer side of the tunnel doesn't generate one automatically, you can create one using the Generate option.

h) Select the **Routing Option.**

i) Create a **Cloud Router,** by entering the details. Click **Save and Continue.**

Step 3 Create a **Cloud Router.**

a) Enter **Google ASN.**

The private ASN (64512 - 65534, 4200000000 - 4294967294) for the router you are configuring. It can be any private ASN you are not already using. For example, 65002.

AWS creates 2 tunnel interfaces for redundancy. If you do not specify details, AWS randomly generates tunnel options.

Step 4 Enter **BGP** session details.

a) Enter name of the BGP.

b) Enter **Peer ASN.**

The private ASN (64512 - 65534, 4200000000 - 4294967294) for the router you are configuring. It can be any private ASN you are not already using. For example, 65001.

c) Enter **Google BGP IP address.**

The BGP interface IP addresses must be link-local IP addresses belonging to the same /30 subnet in 169.254.0.0/16. For example, 169.254.1.1.

d) Enter **Peer BGP IP address**

AWS creates 2 tunnel interfaces for redundancy. If you do not specify details, AWS randomly generates tunnel options.

5. Click **Create.**

This create the gateway, cloud router, and all the tunnels. Remember that the tunnels will not connect until the peer router is configured.

What to do next

Configure the firewall rules for VPN to allow inbound traffic from the peer network subnets.

Creating a VPN Connection Using Static Routing

Follow the procedure given below to create a customer gateway:

Step 1 From the GCP console, go to the **VPN** page.

Step 2 Click **Create VPN Connection.**

The Create VPN Connection window is displayed. Enter the following details:

a) Name of the **VPN** gateway.

b) Select the **VPC** network.

The network containing the instances the VPN gateway is going to serve. Ensure this network does not conflict with your on-premises networks.

c) Select the **Region.**

The region to locate the VPN gateway. Normally, this is the region that contains the instances you wish to reach.

d) Enter the **IP address.**

Select a pre-existing static external IP address. If you don't have a static external IP address, create one by clicking New static IP address from the drop-down menu.

e) Enter the **Peer IP address.**

Public IP address of the peer gateway.

f) Enter **IKE** version.

IKEv2 is preferred, but IKEv1 is supported if that is all the peer gateway can manage.

g) Enter the **Shared Secret.**

Character string used in establishing encryption for that tunnel. You must enter the same shared secret into both VPN gateways. If the VPN gateway device on the peer side of the tunnel doesn't generate one automatically, you can create one using the Generate option.

h) Enter the **Remote Network IP** range.

For example, 10.0.0.0/8. The range, or ranges, of the peer network, which is the network on the other side of the tunnel from the Cloud VPN gateway you are currently configuring.

i) Specify the **Local Subnet.**

Specifies which IP ranges are routed through the tunnel. This value cannot be changed after the tunnel is created because it is used in the IKE handshake.

j) Specify the **Gateway Subnet.**

You can leave it blank as the local subnet is the default option.

k) Enter the **Local IP** ranges.

You can leave it blank except for the gateway's subnet.

Step 3 Click **Create**.

This create the gateway, and initiates all the tunnels. Remember that the tunnels will not connect until the peer router is configured.

What to do next

Configure the firewall rules for VPN to allow inbound traffic from the peer network subnets.

Create Firewall Rules

Firewall rules allow inbound traffic from the peer network subnets, and you must configure the peer network firewall to allow inbound traffic from your Compute Engine prefixes.

To enable traffic to pass to a VM instance, create a firewall rule:

Step 1 From the navigation menu in the Google Cloud Platform Console, scroll down to **VPC network** and select **Firewall Rules**.

Step 2 Click **CREATE FIREWALL RULE** and enter the details.

a) Enter **Name** of the firewall rule.

b) Enter **VPC Network**.

c) Enter **Source** filter.

Choose to filter the traffic using up to four different source filter types.

For example, if you choose to specify a source IP range, you can enter 0.0.0.0/0 to select any IP address.

d) Enter **Source IP ranges**

0.0.0.0/0 (selects all IP ranges in the network).

e) Enter allowed protocols and ports.

A protocol and port range.

String multiple protocol and port ranges together. For example: "icmp", "udp:4789-4790", "tcp:0-6553".

Step 3 Click **Create**.

Creates a firewall rule. To add another firewall rule, repeat the previous steps.

Installing Controller on GCP

Use the following procedure to deploy a controller instance on GCP:

Before you begin

The following prerequisites apply when deploying a controller on GCP:

- An user account or subscription with GCP.
- A Cloud Identity and Access Management (IAM) user.
- A VPC.
- Subnets.
- A security group.
- A VPN connection.
- For every remote site, create:
  - A customer gateway
  - A VPN connection

Step 1 Click **Compute Engine** and **VM instances**.

Step 2 Click **CREATE INSTANCE**.

Select a boot disk to create a new controller VM instance (from "OS images" or custom images) and enter values for the following fields.

a) Specify **Name**.

Name for your VM, using only lowercase letters.

b) Specify **Region**.

c) Specify **Zone**.

A zone is often a data center within a region.

d) Select a **Machine type**.

Supports Small (4 CPU, 8GB RAM), Medium (8 CPU, 16 GB RAM) and Large (16 CPU, 32 GB RAM) profiles.

e) (Optional) Click **Customize** to select the number of cores(vCPUs), memory size, and GPUs.

Step 3 Leave container unselected.

Step 4 Click **Change** on the Boot disk.

Step 5 Go to **OS images** tab and select the required image using radio buttons.

Note
- The custom image is required only during the initial instance.
- Do not change the boot disk.

Step 6 Click **Select**.

Step 7 In the **Firewall** section, select either **Allow HTTP traffic** or **Allow HTTPS traffic** to access Web UI.

Step 8 In the **Deletion protection** section, check the **Enable deletion protection** checkbox to prevent the instance from getting deleted.

Step 9 In the **Automation** section, specify the **Startup** script.

This allows you to run scripts when your instance boots up or restarts.

Use this section to add the *username* and *password* to access the instance.

When you specify a Cisco IOS command, use escape characters to pass special characters that are within the command: ampersand(&), double quotes("), single quotes('), less than(<) or greater than(>). An example is provide below:

```
Section: IOS configuration
hostname mylc
username cisco privi 15 pass 0 cisco
!If you want to add more IOS commands, you can add here
Section: delete
Section: Python package
```

Step 10 Click **Networking** tab from the **Management, Security, Disks, Networking, Sole Tenancy** section.

Step 11 Add SSH-key information in the **Network tags**.

Step 12 Click **Add network interface**.

Step 13 In the **Networking Interfaces** dialog box, select the default interface.

For example, the default security group is 10.142.0.0/20.

Step 14 In the **Networking Interface** window, select the first *default* interface.

Step 15 Set **IP Forwarding** to On.

This prevents the traffic from being blocked.

Step 16 Set **Primary internal IP** as Ephemeral (automatic).

This private IP address is obtained automatically from the selected subnet.

Step 17 Specify **External IP** as Ephemeral (automatic).

You can use this public IP address when you start an SSH session from a *terminal* server. You may also choose to specify this External IP address as static. The external IP address of each interface is either ephemeral or static.

Step 18 Click **Done**.

Creates the first interface.

Step 19 Click **Create**.

The newly created controller VM instance boots up. It may take a few minutes to complete the boot process.

Accessing Controller Instance on GCP

After completing the configuration, you can connect to the controller using SSH. For that you need private key of the SSH.

Follow the procedure given below to access the controller on GCP using SSH:

- Enter the command: ssh -i *private-key-file-path username-in-key@ip-address-of-eth1*
- Or, Login using Username and Password that was created using the IOS command during the boot: ssh *username@ip-address-of-eth1*

CHAPTER 7

Installing the Controller in Microsoft Hyper-V Hypervisor

Microsoft Hyper-V Support Information

The Catalyst 9800-CL Cloud Wireless Controller installation on Microsoft Hyper-V requires the manual creation of a VM and installation, using the .iso file.

The following Microsoft Hyper-V features are supported:

- Snapshot
- Export
- Hyper-V Replica

For more information about Microsoft Hyper-V, see the Microsoft documentation.

Note While running Microsoft Hyper-V VM, you may get the following traceback log continuously in the console:

```
"PLATFORM_INFRA-3-TOO_INTR_OVER_LIMIT_HIGH_RISK: IOS thread blocked due to SYSTEM LEVEL
ISSUE"
```

To avoid this issue, perform the following steps:

1. Configure the controller in serial mode, using the commands given below.

```
Device# configure terminal
Device(config)# platform console serial
Device(config)# end
Device# reload
```

2. Run the following command:

```
PS C:\> Set-VMComPort TestVM 1 \\.\pipe\TestPipe
```

3. Use Putty in administrative mode to access the console.

Installation Requirements for Microsoft Hyper-V

Before installing the controller on a Microsoft Hyper-V VM, the following must be installed on the host:

- Hyper-V Manager
- Failover Cluster Manager
- Virtual Switch

Note We recommended that you create the Virtual Switch prior to creating the VM.

The hardware profiles and the recommended resources are listed in the table given below:

Table 31: Hardware Requirements

Settings	Small	Medium	Large
Minimum Number of vCPUs	4	6	10
Minimum Memory	8 GB	16 GB	32 GB
Required Storage	16 GB	16 GB	16 GB
Minimum Number of vNICs	2	2	2
Maximum Access Points	1000	3000	6000
Maximum Clients Support	10,000	32,000	64,000

Creating the VM

To create the VM, perform the following steps:

Note You can install the controller on Microsoft Hyper-V using Microsoft Hyper-V Manager or Microsoft System Center VMM.

Step 1 In Hyper-V Manager, click on the host.

Step 2 Select **New > Virtual Machine.**

Step 3 Click **Specify Name and Location.**

- Enter the name of the VM.
- (Optional) Click the checkbox to store the VM in a different location.

Step 4 Click **Next.**

Step 5 On the **Specify Generation** screen, specify the generation of the machine to be loaded.

Note The choice of Generation 1 or Generation 2 depends on your requirements. Generation 2 supports advance features like boot from Small Computer System Interface (SCSI), secure boot, higher hardware limits, Unified Extensible Firmware Interface (UEFI) BIOS, GUID Partition Table (GPT) partitioning, and so on. If Generation 2 is selected, unselect the **Enable Secure Boot** checkbox after the deployment, as the controller does not support secure boot.

Step 6 On the **Assign Memory** screen, enter the **Startup Memory** value.

The controller requires 8196 MB for the startup memory.

Step 7 Click **Next.**

Step 8 On the **Configure Networking** screen, select a network connection to the virtual switch that was previously created.

The network adapter selected in this step will become the first interface for the controller when the VM is launched and the router boots. The other vNICs for the VM are created in the next procedure.

Step 9 Click **Next.**

Step 10 On the **Connect Virtual Hard Disk Screen,** select the following option:

- Attach a virtual hard disk later.

Note The New Virtual Machine Wizard only supports creating a virtual hard disk using the .vhdx format. The controller requires that the hard disk uses the .vhd format. Create the virtual hard disk after the VM has been created.

Click **Next.** The **Summary** screen is displayed.

Step 12 Review the VM settings, and if it is looking good, click **Finish.**

The new VM is created.

Configuring the VM Settings

To configure the VM settings before launching the VM, perform the following steps:

Before you begin

Before launching the instance, add the network adapters (as required), disk, and load the .iso image in to the disk drive.

We recommended that you create and use separate network interfaces for Management, Wireless Management and High Availability. In case of HA deployments, create 3 network interfaces and attach the VM to the appropriate networks. For non-HA deployments, create 2 network interfaces.

The creation of management, wireless management and HA networks should be done before launching VM. The IP addressing on these interfaces could be either static or DHCP and should be configured as part of the bootstrap configuration.

The order in which the networks are attached to the interface is important as the first network attached is used for Management, second for Wireless Management (unless configured explicitly) and third for the HA.

Step 1 In Hyper-V Manager, select the host, and then right-click on the VM that was created in the previous steps.

Step 2 Select **Settings.**

Step 3 Specify the number of virtual processors, also known as virtual CPUs (vCPUs) for the VM.

Step 4 Under **IDE Controller 0,** select the Hard Drive.

Click the **Virtual Hard Disk** checkbox and click **New** to create a new virtual hard disk.

The New Virtual Hard Disk Wizard opens. Click **Next.**

a) On the **Choose Disk Format** screen, click the VHD checkbox to create the virtual hard disk using the .vhd format. Click **Next.**
b) On the **Choose Disk Type** screen, click on the **Fixed Size** option. Click **Next.**
c) Specify the Name and Location for the virtual hard disk. Click **Next.**
d) On the **Configure Disk** screen, click the option to create a new blank virtual hard disk. For the size, specify 16 GB.
e) Click **Next** to view the Summary of the virtual hard disk settings.
f) Click **Finish** to create the new virtual hard disk.

When the new hard disk has been created, continue configuring the VM settings with the next step.

Step 5 Under IDE Controller1, select the **DVD Drive.**

The **DVD Drive** screen is displayed.

For the **Media** setting, click the **Image File** checkbox, and browse to the .iso file that you downloaded from Cisco.com.

Step 6 Click **Ok.**

Step 7 Select **Network Adapter** to verify that the network connection to the virtual switch is configured.

Step 8 Select **Com 1** to configure the serial port.

This port provides access to the controller console.

Step 9 Select **Hardware > Add Hardware** to add the network interfaces (vNICs) to the VM.

a) Select **Network Adapter** and click **Add**.

Microsoft Hyper-V adds the network adapter and highlights that hardware with the status Virtual Switch "Not Connected".

b) Select a virtual switch on the drop-down menu to place the network adapter onto it.

Repeat these steps for each vNIC. The controller supports only the HV NETVSC vNIC type. The maximum number of vNICs supported is 8.

Note The hot-add of vNICs is not supported with Microsoft Hyper-V, so the network interfaces need to be added before launching the VM.

After the controller boots, you can verify the vNICs and how they are mapped to the interfaces using the **show platform software vnic-if interface-mapping** command.

Step 10 Click **BIOS** to verify the boot sequence for the VM.

The VM should be set to boot from the CD.

Launching the VM to Boot the Controller

To launch the VM, perform the following steps:

Step 1 Select the virtual switch.

Step 2 Select the VM and click **Start**.

The Hyper-V Manager connects to the VM, and starts the launch process. Once the VM is launched, the controller starts the boot process

Configuring Tagged Ports

The tagged port configuration is done on the host OS. By default, the VLAN tagged packets are dropped at the host OS at the vNIC. To allow these packets through to the controller, set the specific vNIC on the controller as tagged.

Note If you use GUI to create network interfaces, you cannot specify interface names and all the interfaces will be named as Network Adapter. So, using these commands, all the network adapters in the controller can be converted to tagged.

These commands are to be entered in a Power Shell.

Step 1 To see the list of adapters and assignment, use the following script:


```
Get-VMNetworkAdapter -VMName <C9800-name>
```

Note To rename the adapter name, use the following command:

```
Rename-VMNetworkAdapter -VMName <C9800-name> -Name "<C9800-adapter-name>" -NewName "Eth1"
```

Here, **Eth1** is the adapter name.

Step 2 To configure Ethernet1 (data port/management) as Trunk, with Native VLAN id as 0, use the following script:

```
Set-VMNetworkAdapterVlan -VMName "C9800" -VMNetworkAdapterName Eth1 -Trunk -AllowedVlanIdList "1-4000"
-NativeVlanId 0
```

Step 3 To configure Ethernet0 (serial port) as access or untagged, use the following script:

```
Set-VMNetworkAdapterVlan -VMName "C9800" -VMNetworkAdapterName Eth0 -Untagged
```

Step 4 Enable MAC address spoofing to allow the trunk port to pass the tagged traffic.

To enable MAC address spoofing, perform the following:

a. Select the virtual machine and select **Actions > Settings**.

b. Expand **Network Adapter** and select **Advanced Features**.

c. Select **Enable MAC Address spoofing**.

Creating a Bootstrap Day0 Configuration

The following steps are performed on the Linux server.

Step 1 Create **iosxe_config.txt** or **ovf-env.xml** file.

Step 2 Create a disk image from this file using the command:

```
mkisofs -l -o ./c9800_config.iso <configuration_filename>
```

Step 3 Mount the c9800_config.iso as an additional disk during creation of the virtual machine and power on the VM.

CHAPTER 8

Booting the Controller and Accessing the Console

Day 0 WebUI Wizard for Public Cloud

Follow the procedure given below to create a Day 0 configuration and push it to the controller:

Step 1 In the address bar of a web browser, enter the **IP address** of the controller.

Step 2 Enter the **Username** and **Password**.

This displays the **Configuration Setup Wizard** window.

Enter the details in **General Settings** window.

a) Select the **Deployment Mode**.
b) Select the **Country**.
c) Select the **Date**.
d) Enter the **Time** or select the **Timezone** using the drop down list.
e) Enter the **NTP Servers** name.
f) Enter the **AAA Servers** name.

Step 3 Enter the **Wireless Management Settings**:

a) Choose **Port Number**.
b) Choose **IP Address**.

Step 4 Click **Next**.

Step 5 Enter the **Wireless Network Settings**:

a) Enter a **Network Name**.
b) Select the **Network Type**.
c) Select the **Security** option using the drop-down.
d) Enter the **Pre-Shared Key**.

e) Click **Add**.

Note Enter three wireless network settings, one for wireless management, another for device management and one more for guest management.

Step 6 Click **Next**.

This opens the Advanced Settings page.

Step 7 Enter the details in **Advanced Settings** page.

a) Select the **Client Density** using the slider.
b) Enter the **RF Group Name**.
c) Use the drop-down to select **Traffic Type**.
d) Enter the **Virtual IP Address**.
e) Use the **Generate Certificate** slider to generate certificates for APs.

This certificate is required for APs to join the controller.

f) Use the drop-down to select **RSA Key-Size**.
g) Enter the **Signature Algorithm**.
h) Enter the **Password**.
i) Review the details in **Summary** page.

Step 8 Click **Finish**.

Step 9 Click **Yes**.

This creates the configuration and pushes it to the controller.

Day 0 WebUI Wizard for Private Cloud

Follow the procedure given below to create a Day 0 configuration and push it to the controller:

Step 1 n the address bar of a web browser, enter the **IP address** of the controller.

Step 2 Enter the **Username** and **Password**.

This displays the **Configuration Setup Wizard** window. Enter the details in the **General Settings** window.

a) Select the **Deployment Mode**.
b) Select the **Country**.
c) Select the **Date**.
d) Enter the **Time** or select the **Timezone** using the drop down list.
e) Enter the **NTP Servers** name.
f) Enter the **AAA Servers** name.

Step 3 Enter the **Service Port Settings**:

a) Choose **DHCP**.
b) Enter the **Static IP** address.
c) Enter the **Subnet Mask**.

Step 4 Enter the **Static Route Settings (Optional)**:
a) Enter the **IP Address**.
b) Enter the **Subnet Mask**.
c) Enter the **Gateway** address.

Step 5 Enter the **Wireless Management Settings**:
a) Choose **Port Number**.
b) Enter the **VLAN**.
c) Choose **IPv4** or **IPv6**.
d) Enter the **Wireless Management IP** address.
e) Enter the **Subnet Mask**.
f) Enter the **Management VLAN DHCP Server**.

Step 6 Click **Next**.

This opens the Wireless Network Settings page.

Step 7 Enter the **Wireless Network Settings**:
a) Enter a **Network Name**.
b) Select the **Network Type**.
c) Select the **Security** option using the drop-down.
d) Enter the **Pre-Shared Key**.
e) Click **Add**.

Note Enter three wireless network settings, one for wireless management, another for device management and one more for guest management.

Step 8 Click **Next**.

This opens the Advanced Settings page.

Step 9 Enter the details in **Advanced Settings** page.
a) Select the **Client Density** using the slider.
b) Enter the **RF Group Name**.
c) Use the drop-down to select **Traffic Type**.
d) Enter the **Virtual IP Address**.
e) Enter the **Local IP**, **Subnet Mask**, **Remote IP** for High Availability.

Note Available only when the deployment mode is set to ACTIVE.

f) Use the **Generate Certificate** slider to generate certificates for APs.

This certificate is required for APs to join the controller.

g) Use the drop-down to select **RSA Key-Size**.
h) Enter the **Signature Algorithm**.
i) Enter the **AP password**.
j) Review the details in **Summary** page.

Step 10 Click **Finish**.
Step 11 Click **Yes**.

This creates the configuration and pushes it to the controller.

Booting the Controller

The controller boots when the VM is powered on. Depending on your configuration, you can monitor the installation process on the virtual VGA console.

Follow the procedure given below to boot up the controller:

1. Power up the VM. Within 5 seconds of powering up the VM, choose a console described from Step 2 to Step 4 to view the device's bootup and to access the controller CLI.
2. (Optional) Click **Auto Console** to use automatic console detection. This is the default setting, and the controller will boot using automatic console detection if another option is not selected within 5 seconds.
3. (Optional) Click **Virtual Console** to use the virtual VGA console. If you choose to use the virtual console, the rest of the steps in this procedure do not apply. The controller starts the boot process.
4. Use one of the following commands to Telnet to the VM:
   - **telnet://***host-ipaddress:portnumber*
   - **telnet***host-ipaddress portnumber* (from a UNIX xTerm terminal)
5. After booting, the system displays the main software image and the Golden image, with an instruction that the highlighted entry is booted automatically in 3 seconds. Do not select the option for the Golden image, and allow the main software image to boot.

Note While doing backup restore of configs, make sure you do not have **platform console serial**, as it could make the controller boot into grub mode and recovery is not possible.

Accessing the Controller Through the Virtual VGA Console

You will be prompted for wireless configuration after the Day 0 banner.

For information on modifying the configuration after you create it, see the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide and the Cisco Catalyst 9800 Series Wireless Controller Command Reference Guide.

This section covers the following:

- Configuring the device management interface.
- Configuring the device management IP.
- (Optional) Setting a static route.
- Configuring the management credentials.

- Configuring the wireless management interface.
- Choosing the deployment mode.
- Configuring the system name or hostname.
- Configuring credentials for management access on access points.
- Configuring the country code.
- Configuring the time using an NTP server or manually.
- (Optional) Configuring a time zone.
- (Optional) Configuring the wireless client density.
- (Optional) Configuring AAA servers.
- (Optional) Configuring the wireless network settings.
- (Optional) Configuring a network name or SSID.
- (Optional) Configuring a virtual IP.
- (Optional) Configuring an RF network name.
- (Optional) Configuring a self-signed certificate.
- (Optional) Configuring high availability.

Note Presently, there is no direct method to get back to your previous configuration. Press **Ctrl-C** to restart the configuration and return to the setup without saving the configuration.

Day 0 CLI Wizard for the Controller

Step 1 You can get into the Day 0 setup wizard using the **write erase** command or directly on the Day 0 device.

Step 2 Device management interface setup configures the device management or service port. This interface enables the basic configuration to access the device using the **GUI**. This is an optional configuration where you can opt to configure only the wireless management interface and not the device management.

```
Configure device management interface?(yes):
```

Note There is no dedicated device management port for Cisco Catalyst 9800-CL Cloud Wireless Controller. So, you are prompted to select one of the options from the given range.

```
Select interface to be used for device management
1. GigabitEthernet1 (Up)
2. GigabitEthernet2 (Up)
3. GigabitEthernet3 (Up)
Choose the interface to config [1]:
```

Step 3 Device management IP helps access the device using the GUI.


```
Configure static IP address? [yes]:
  Enter the interface (e.g.GigabitEthernet1): 192.168.1.10
  Enter the subnet mask (GigabitEthernet1) [255.0.0.0]: 255.255.255.0
```

Step 4 [Optional] Setting a static route to access the device using the GUI.

```
Configure static route? [yes]:
Enter the destination prefix: 192.168.1.0
Enter the destination mask: 255.255.255.0
Enter the forwarding router IP: 192.168.1.1
```

Step 5 Enter the management username and password. This is a mandatory step.

```
Enter the management username: cisco
  Enter the password: ********
  Reenter the password: ********
```

Step 6 Configure the wireless management if you haven't configured a device management interface.

```
Basic management setup is now complete. At this point, it is possible to save the above and
continue wireless setup using the webUI (for this, choose 'no' below)

Would you like to continue with the wireless setup? [yes]: yes
```

Note This prompt is not applicable for 17.4 release.

Note If you have not configured the device management, the setup moves to **Step 7** before displaying the above banner.

In 17.3 release, you will be allowed to exit the wizard after configuring at least one of the interfaces, that is, device or wireless management.

This banner is no longer available in 17.4. You cannot exit the wizard without completing the configuration.

If you select **Yes**, you need to follow the upcoming steps. Also, you can access the device using the IP configured in Step 4.

Step 7 Wireless management interface is a mandatory configuration:

```
Configuring wireless management interface
  Select interface to be used for wireless management
    1. GigabitEthernet2 (Up)
    2. GigabitEthernet3 (Up)
  Choose the interface to config [1]:
```

Note If GigabitEthernet1 is used for device management interface then the remaining GigabitEthernet interfaces will be displayed.

Step 8 Enter a VLAN ID:

```
Enter the vlan ID [1-4094]: 112
```

Step 9 Configure an IPv4 or IPv6 address:

```
Configure ipv4 address? [yes]:
  Enter the interface IP (GigabitEthernet1): 9.11.112.43
```

```
Enter the subnet mask (GigabitEthernet1 [255.0.0.0 | 255.255.255.0]
Configure IPv6 address? [yes|: no
```

Step 10 Configure a VLAN DHCP server and IP address:

```
Do you want to configure a VLAN DHCP Server? [yes|: yes
  Enter the VLAN DHCP Server IP [GigabitEthernet1: 9.11.112.45
```

Step 11 [Optional] Setting a static route to attach an AP client to the controller. The default options for static routes prompts you to configure a default route. However, you can specify a different route as well.

```
Configure static routes [yes|no|]: yes
  Enter the destination prefix [0.0.0.0]:
  Enter the destination mask [0.0.0.0]:
  Enter the forwarding router IP: 9.11.112.1
```

Note If you configure the device as HA RMI and you haven't configured a default route (that is, source and destination as 0.0.0.0), the wizard asks for the default route information.

```
Basic management setup is now complete. At this point, it is possible to save the above and
continue wireless setup using the web UI(the only choice that follows)

Would you like to continue with the wireless setup? [yes]:
```

Step 12 Choose the deployment mode:

```
Choose the deployment mode
   1. Standalone
   2. Active
   3. Standby
Enter your selection [1]:
```

Note You can choose from one of the following deployment modes:

- **Standalone:** In this mode, you do not get to view any high availability pairing information.
- **Active:** In this mode, the controller needs to be configured with all the Day 0 information.
- **Standby:** In this mode, the configuration proceeds to the **High Availability** configuration.

Step 13 Configure the system name or hostname:

```
Enter the hostname [WLC]: cisco-wlc
```

Note This is a mandatory step. The hostname needs to confirm to the RFC standards.

Step 14 [Optional] Configure the login credentials for an AP.

```
Configure credentials for management access to Access Points? [yes|]:
  Enter the management username: user1
  Enter the management password: ****
    Reenter the password: ****
  Enter the privileged mode access password: ****
    Reenter the password: ****
```

Step 15 Configure the country code. You can specify multiple country codes by separating them with a comma.

```
Configure country code for wireless operation in two letters [ |US]:
```


Step 16 Configure the date and NTP to allow access points to join the controller. You can configure time using an NTP server or manually.

Note Enter the date in the following format:

MM/DD/YYYY

```
Configure a NTP server now ? [yes|n]: no

Configure the system time now? [yes|n]: yes

Enter the date in MM/DD/YYYY format: 10/05/2021
Enter the time in HH:MM:SS format: 21:22:23
```

Step 17 [Optional] Configure a timezone:

```
Configure timezone? [yes|n]:
  Enter name of timezone: AM
  Enter hours offset from UTC (-23,23): 5
  Enter mins offset from UTC (0,59) [0]: 30
```

Step 18 [Optional] Configure the expected client density:

```
Configure Wireless client density? [yes|n
  Choose the client density
     1. Low
     2. Typical
     3. High
  Enter your selection [2]: 3
```

Step 19 [Optional] Configure AAA servers:

Note You can configure a maximum of 6 servers during Day-0 configuration.

```
Configure AAA servers? [yes|n]:
  Enter the AAA server address: 9.11.112.46
  Enter the AAA key: ***
Do you want to add more AAA servers? [yes|n]: yes
  Enter the AAA server address: 9.11.112.47
  Enter the AAA key: ***
Do you want to add more AAA servers? [yes|n]: no
```

Note The AAA servers are required for WPA2 Enterprise. In 17.4 release, you need to configure AAA place. If you follow **Step 21**, WPA2 Enterprise will not ask for AAA servers in **Step 22**.

Step 20 [Optional] Configure wireless network settings to configure WLAN information for an AP and client join:

```
Configure wireless network settings? [yes|]:
```

Step 21 [Optional] Configure an SSID for client join:

```
Enter the network name or network SSID identifier (ssid):
Choose the network type
    1. Employee
    2. Guest
```

If you choose **Employee** as the network type, the following options are displayed:


```
Choose the security type
    1. WPA Personal
    2. WPA Enterprise
  Enter your selection [1]:
```

If you choose **WPA2 Personal**, you will need to enter a pre-shared key (ASCII).

```
Enter the pre-shared key (ASCII):
```

If you choose **WPA2 Enterprise**, you will be able to add multiple AAA servers.

```
Enter the AAA server address
Enter the AAA key:
Added more AAA server details? [yes]
```

If you choose **Guest**, you get to view the following options:

```
Please choose the security type:
1. Webauth
2. Webpasswd
3. Consent
4. Webconsent
Enter the security type:
```

Step 22 [Optional] Configure a virtual IP address. The default virtual IP address is 192.0.0.1.

```
Configure virtual IP? [yes|]:
  Enter the virtual IP [192.0.0.1]:
```

Step 23 [Optional] Configure an RF network name.

```
Configure RF-Network name? [yes|n]:
  Enter the RF-Network Name: mlabcdf
```

Step 24 [Optional] Configure a self-signed certificate.

```
Auto generate certificate for AP (y/n) [yes|n]:
Choose key size
1.2048
2.3072
3.4096
Enter your selection [1]:
Choose the signature algorithm
1.SHA256
2.SHA384
Enter your selection [1]:
Enter secret key(minimum 8 characters): ********
Self Signed certificate generation will be done after system boot up.
```

Step 25 [Optional] Configure high availability.

If you choose the deployment mode as Active or Standby, you will need to choose from one of the HA pairing type:

a. RMI

b. RP-RP

Note For information on HA pairing types, see Part: **High Availability** | **High Availability > Information About Redundancy Management Interface** in *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.4.x.*

```
High Availability configuration
  Please choose the HA pairing type
    1. RMI
    2. RP-RP
  Enter your selection [1]:
```

If you choose RMI-RP, you need to select an interface to be used as redundancy port:

```
Select interface to be used as redundancy port
  1. GigabitEthernet3 (UP)
Choose the interface to config [1]: 1
Enter the RMI IP for local chassis: 9.11.112.50
Enter the RMI IP for remote chassis: 9.11.112.51
Enter the gateway IP of the link (peer): 9.11.112.1
```

If you choose the deployment mode as Standby, you need to specify the VLAN ID for completing the pairing:

```
  Enter the RMI IP for local chassis: 9.11.112.51
  Enter the RMI IP for remote chassis: 9.11.112.50
  Enter the wireless management VLAN: 112
```

If you choose RP, you need to select an interface to be used as redundancy port:

```
Select interface to be used as redundancy port
  1. GigabitEthernet3 (UP)
Choose the interface to config [1]: 1
Enter the local IP:
Enter the peer mask:
Enter the remote IP:
```

Note It is recommended to use GigabitEthernet0 for device management interface, GigabitEthernet2 for wireless management interface, and GigabitEthernet3 for HA.

CHAPTER 9

Upgrading the Software

Prerequisites for the Software Upgrade Process

This section describes how to upgrade the Cisco IOS XE software for an existing controller installation on a VM.

Note
- This procedure provides details about upgrading to a new software version of the controller on the same VM.
- We recommend that you use Web UI method for a faster upgrade process.

Be sure to complete the following prerequisites before upgrading the Cisco IOS XE version of the controller software image:

- Compatibility with the hypervisor vendor and version being used. If you want to upgrade to a new hypervisor version that is not supported by your current version of controller, you need to upgrade the version of controller before upgrading to the new hypervisor version.
- Memory requirements of the VM for the controller software image:
  - If the new controller version requires more memory than your previous version, you must increase the memory allocation on the VM before starting the upgrade process.
  - You must use the **.bin** file to upgrade or downgrade your software. Use the **.iso** and **.ova** files for first-time installation only.

Upgrading the Controller Software (CLI)

Follow these instructions to upgrade from one release to another, in install mode.

Before you begin

- Clean up the old installation files using the **install remove inactive** command.
- For upgrading the software using CLI, we recommend that you use install mode for the upgrade. Use the **show version** command to verify the boot mode.
- To perform a software image upgrade, you must be booted into IOS through **boot flash:packages.conf**.
- Ensure that boot parameter is set to boot only from *flash:packages.conf*.

Step 1 Go to the software download page: https://software.cisco.com/download/home/286316412/type

a) Click IOS XE Software link.

b) Select the release number you want to install.

Note Cisco recommended release is selected by default. For information on release designations, see this link: https://software.cisco.com/download/static/assets/i18n/reldesignation.html?context=sds

c) Click **download**.

Step 2 Copy the new image to flash by running the following command: **copy tftp:***image* **flash:**

Note Transferring large files over TFTP is a time-consuming process

```
Device# copy tftp://10.8.0.6//C9800-universalk9_wlc.xx.xx.xx.SPA.bin flash:

Destination filename [C9800-universalk9_wlc..xx.xx.xx..SPA.bin]?
Accessing tftp://10.8.0.6//C9800-universalk9_wlc.xx.xx.xx.SPA.bin...
Loading /C9800-universalk9_wlc.xx.xx.xx.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]

601216545 bytes copied in 50.649 secs (11870255 bytes/sec)
```

Step 3 Verify that the image has been successfully copied to flash by running the following command: **dir flash:**

```
Device# dir flash:*.bin
```

Step 4 Install the software image to flash by running the following command: **install add file bootflash:***image* **activate commit**

Note You can also use multi-step installation of the software. To perform multi-step installation, go to Step 5.

```
Device# install add file bootflash:C9800-universalk9_wlc.xx.xx.xx.SPA.bin activate commit

install_add_activate_commit: START Thu Dec  6 15:43:57 UTC 2018
Dec  6 15:43:56.609 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install one-shot
bootflash:C9800-xx-universalk9.xx.xx.xx.SPA.bin
install_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying bootflash:C9800-xx-universalk9.xx.xx.xx.SPA.bin to the selected chassis
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
  [1] Add package(s) on chassis 1
  [1] Finished Add on chassis 1
```



```
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

Image added. Version: xx.xx.xx.216
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/bootflash/C9800-xx-rpboot.xx.xx.xx.SPA.pkg
/bootflash/C9800-xx-mono-universalk9.xx.xx.xx.SPA.pkg

This operation requires a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on all members
  [1] Activate package(s) on chassis 1
    --- Starting list of software package changes ---
    Old files list:
      Removed C9800-xx-mono-universalk9.BLD_Vxxxx_THROTTLE_LATEST_20181022_153332.SSA.pkg
      Removed C9800-xx-rpboot.BLD_Vxxxx_THROTTLE_LATEST_20181022_153332.SSA.pkg
    New files list:
      Added C9800-xx-mono-universalk9.xx.xx.xx.SPA.pkg
      Added C9800-xx-rpboot.xx.xx.xx.SPA.pkg
    Finished list of software package changes
  [1] Finished Activate on chassis 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
  [1] Commit package(s) on chassis 1
  [1] Finished Commit on chassis 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Thu Dec  6 15:49:21 UTC 2018
Dec  6 15:49:21.294 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install one-shot
 PACKAGE bootflash:C9800-xx-universalk9.xx.xx.xx.SPA.bin
```

Note The system reloads automatically after executing the **install add file activate commit** command. You do not have to manually reload the system.

Step 5 (Optional) You can also perform multi-step installation of the software:

Note Ensure that boot parameter is set to boot only from *flash:packages.conf*.

a) Add the controller software image to the flash and expanded it, using the **install add file** command.

```
Device# install add file bootflash:C9800-universalk9_wlc.xx.xx.xx.SPA.bin
```

b) Perform predownload of the AP image, using the **ap image predownload** command.

```
Device# ap image predownload
```

c) Check the predownload status of the AP, using the **show ap image** command.

```
Device# show ap image
```

d) Activate the package, using the **install activate** command.

```
Device# install activate
```


e) Commit the activation changes to be persistent across reloads using the **install commit** command.

```
Device# install commit
```

Step 6 Verify the installation by running the following command: **show version**

Note When you boot the new image, the boot loader is automatically updated, but the new bootloader version is not displayed in the output until the next reload.

Step 7 To see a summary of the active packages in a system, run the following command: **show install summary**

```
Device# show install summary

[ Chassis 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   I    <v1>
IMG   C    <v2>
```

Upgrading the Controller Software (GUI)

Before you begin

Clean up the old installation files using the **Remove Inactive Files** link.

Note For GUI options such as *Software Maintenance Upgrade*, *AP Service Package*, and *AP Device Package*, see the respective feature sections.

Step 1 Choose **Administration > Software Management**.

Step 2 Choose an option from the **Upgrade Mode** drop-down list:

- **INSTALL**: The Install mode uses a package-provisioning file named *packages.conf* in order to boot a device.
- **BUNDLE**: The Bundle mode uses monolithic Cisco IOS images to boot a device. The Bundle mode consumes more memory than the Install mode because the packages are extracted from the bundle and copied to RAM.

Note You get to view the **Destination** field only for BUNDLE upgrade mode.

Step 3 From the **Transport Type** drop-down list, choose the transfer type to transfer the software image to your device as **TFTP**, **SFTP**, **FTP**, **Device**, or **Desktop (HTTP)**.

- If you choose **TFTP** as the **Transport Type**, enter the **Server IP Address** of the TFTP server that you want to use. Also, enter the complete **File Path**.

  In controllers, the IP TFTP source is mapped to the service port by default.

62

- If you choose **SFTP** as the **Transport Type**, enter the **Server IP Address** of the SFTP server that you want to use. Also, enter the **SFTP Username**, **SFTP Password**, and the complete **File Path**.
- If you choose **FTP** as the **Transport Type**, enter the **Server IP Address** of the FTP server that you want to use. Also, enter the **FTP Username**, **FTP Password**, and the complete **File Path**.
- If you choose **Device** as the **Transport Type**, choose the **File System** from the drop-down list. In the **File Path** field, browse through the available images or packages from the device and select one of the options, and click **Select**.
- If you choose **Desktop (HTTPS)** as the **Transport Type**, choose the **File System** from the drop-down list. In the **Source File Path** field, click **Select File** to select the file, and click **Open**.

Step 4 Click **Download & Install**.

Step 5 To boot your device with the new software image, click **Save Configuration & Reload**.

Rebooting the Controller

After you have copied the new system image into the bootflash memory, loaded the new system image, and saved a backup copy of the new system image and configuration, reboot the VM using the **reload** command.

Note When you reload an active device, it reloads the whole stack.

For more information about rebooting the VM, see your VMware documentation.

After rebooting, the controller VM must include the new system image with a newly installed Cisco IOS XE software version.

Note After an upgrade from 16.11 to an higher release, you should be able to view the new login page.

If not, perform either one of the following to redirect to the login page:

- Refresh GUI.
- Clear cache.

CHAPTER 10

License Information

Evaluation License

The wireless controller operates on evaluation mode when the device is not registered. The evaluation mode is for 90 days. After the expiry of the evaluation period, if the wireless controller is not registered to a smart account, the wireless controller will start displaying syslog evaluation expiration messages. These error messages are purely for informational purpose only and will not affect the functionality of the wireless controller.

The number of APs supported on the wireless controller when the wireless controller is on EVAL mode will be equal to the capacity of the wireless controller and the wireless controller will be fully operational. No other license is required to use the wireless controller in evaluation mode.

Viewing License Information

Use the **show license udi** command to determine the Universal Device Identifier (UDI) information of your chassis. This may be required at the time of purchasing a new license.

The following example displays sample output from the **show license udi** command:

```
Device# show license udi
SlotID       PID              SN                UDI
-------------------------------------------------------------------------------
*        C9800-CL             xxxxxxxxxx        C9800-CL:xxxxxxxxxx
```

Viewing the Cisco IOS License Level

Use the **show version** command to determine the Cisco IOS license level in the controller.

Example:

```
WLC# show version | section License
License Level: adventerprise
License Type: Smart License is permanent
License Level: adventerprise
AIR License Level: AIR DNA Advantage
```



```
documentation or "License Notice" file accompanying the IOS-XE software.
License Type: Smart License is permanent
License Level: adventerprise
AIR License Level: AIR DNA Advantage
```

Table 11: Show version Command Output Description

Field Name	Description
License Level: adventerprise	Indicates the current Cisco IOS license code level.
License Type: Smart License is permanent	Indicates the type of license that is used. This example shows that the Cisco Smart license is used that provides floating licenses for your user account. Other license types could be: Permanent (purchased) license or an Evaluation 60-day license.
AIR License Level: AIR DNA Advantage	Indicates the AIR network advantage license level.

Use the **show running-config** command or the **show startup-config** command to view the license-level information. The following example displays sample output from the **show running-config** command:

```
WLC# show running-config
.
.
.
license boot level adventerprise
```

Table 12: show running-config Command Output Description

Field Name	Description
license boot level adventerprise	Indicates the current requested Cisco IOS license level to boot.

CHAPTER 11

Troubleshooting

Verifying the Hardware and VM Requirements

To help troubleshoot issues with the controller, make sure that the device is installed on the supported hardware and the following VM requirements are being met:

- Verify that the server hardware is supported by the hypervisor vendor. If you are using VMware, verify that the server is listed in the VMware Hardware Compatibility List. For more information, see the VMware documentation set.
- Verify that the I/O devices, for example, Fibre Channel (FC), Internet Small Computer System Interface (iSCSI), and SAS that are being used are supported by the VM vendor.
- Verify that sufficient RAM is allocated on the server for the VMs and the hypervisor host.
- If you are using VMware, make sure the server has enough RAM to support both VMs and VMware ESXi.
- Verify if the hypervisor version is supported by the controller or not.
- Verify that the correct VM settings are configured based on the amount of memory, number of CPUs, and disk size.
- Verify that the vNICs are configured using a supported network driver.

Network Connectivity Issues

To troubleshoot network connectivity issues for the controller, ensure that the following requirements are met:

- Promiscuous mode should be set to accept to see the traffic sent and received through the vSwitch. Tagged traffic will not flow properly without this mode.
- Verify that there is an active and unexpired license installed on the VM. Enter the **show license** command. The **License State** should be shown as **Active, In Use.**
- Verify that the vNIC for the VMs are connected to the correct physical NIC or to the proper vSwitch.
- Ensure that the vSwitch is configured with the correct VLAN, if you are using virtual LANs (VLANs).
- Ensure that there are no duplicate MAC addresses, if you are using static MAC addresses or VMs that are cloned.

Caution Duplicate MAC addresses might cause the controller feature license to become invalidated, which will disable the device interfaces.

VM Performance Issues

The controller operates within a set of supported VM parameters and settings to provide certain levels of performance that have been tested by Cisco.

Use vSphere Client to view data and troubleshoot VM performance. If you are using vCenter, you can view historical data. If you are not using vCenter, you can view live data from the host.

Ensure that the following requirements are met to troubleshoot performance issues:

- Verify that the device is configured for the correct MTU setting.
- By default, the maximum MTU setting on the device is set to 1500. To support jumbo frames, you need to edit the default VMware vSwitch settings. For more information, see the VMware vSwitch documentation.
- The controller does not support memory sharing between VMs. On the ESXi host, check the memory counters to determine the used and shared memory on the VM. Verify that the counters used by the balloon and swap are zero.
- If a given VM does not have enough memory to support the controller, increase the size of the VM's memory. Insufficient memory on the VM or the host might cause the controller console to hang and be nonresponsive.

Caution When troubleshooting performance issues, note that other VMs on the same host as the controller can impact the performance of the controller VM. Verify that the other VMs on a host are not causing memory issues that impact the controller VM.

- Verify that no network packets are being dropped. On the ESXi host, check the network performance and view the counters to measure the number of receive and transmit packets dropped.

CHAPTER 12

Finding Support Information for Platforms and Cisco Software Images

Support Information for Platforms and Cisco Software Images

Cisco software is packaged in feature sets consisting of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco software images are included in a release. To identify the set of software images available in a specific release or find if a feature is available in a given Cisco IOS XE software image, you can use the Cisco Feature Navigator, Software Advisor, or the corresponding Release Notes document.

For all Cisco Wireless Controller software-related documentation, see:

https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/tsd-products-support-series-home.html

Using Cisco Feature Navigator

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.

You need not be a registered user on Cisco.com to access this tool.

Using the Software Advisor

To determine if a feature is supported by a Cisco IOS XE release, locate the software document for that feature, or check the minimum Cisco IOS XE software requirements with your device. Cisco maintains the Software Advisor tool on Cisco.com at: http://tools.cisco.com/Support/Fusion/FusionHome.do

You must be a registered user on Cisco.com to access this tool.

63

Cisco Catalyst 9200 Series Switches Hardware Installation Guide

First Published: 2018-11-19
Last Modified: 2020-11-17

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Product Overview

Switch Models

The Cisco Catalyst 9200 Series switches have four modular (C9200) and eight fixed (C9200L) switch models. The following tables describe all the available Cisco Catalyst 9200 Series switches and the features supported.

Table 1: C9200L Switch Models and Descriptions

Switch Model	Description
C9200L-24P-4G	Stackable 24x1G PoE+ ports; 4x1G SFP fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24P-4X	Stackable 24x1G PoE+ ports; 4x10G SFP+ fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24T-4G	Stackable 24x1G ports; 4x1G SFP fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24T-4X	Stackable 24x1G ports; 4x10G SFP+ fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48P-4G	Stackable 48x1G PoE+ ports; 4x1G SFP fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48P-4X	Stackable 48x1G PoE+ ports; 4x10G SFP+ fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48T-4G	Stackable 48x1G ports; 4x1G SFP fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48T-4X	Stackable 48x1G ports; 4x10G SFP+ fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.

Switch Model	Description
C9200L-24PXG-4X	Stackable 8xMultigigabit Ethernet PoE+ ports and 16x1G PoE+ ports; 4x10G SFP+ fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-24PXG-2Y	Stackable 8xMultigigabit Ethernet PoE+ ports and 16x ports; 2x25G SFP28 fixed uplink ports; 2 power supply s fans; supports StackWise-80.
C9200L-48PXG-4X	Stackable 12xMultigigabit Ethernet PoE+ ports and 36x1G PoE+ ports; 4x10G SFP+ fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48PXG-2Y	Stackable 8xMultigigabit Ethernet PoE+ ports and 40x1G PoE+ ports; 2x25G SFP28 fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48PL-4G	Stackable 48x1G PoE+ ports with partial PoE support; 4x1G SFP fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.
C9200L-48PL-4X	Stackable 48x1G PoE+ ports with partial PoE support; 4x10G SFP fixed uplink ports; 2 power supply slots; 2 fixed fans; supports StackWise-80.

Table 2: C9200 Switch Models and Descriptions

Switch Model	Description
C9200-24P	Stackable 24x1G PoE+ ports; 4x1G and 4x10G network modules for uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-24PB	Stackable 24x1G PoE+ ports; 4x1G and 4x10G network modules for uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-24T	Stackable 24x1G ports; 4x1G and 4x10G network modules for uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-48P	Stackable 48x1G PoE+ ports; 4x1G and 4x10G network modules for uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-48PB	Stackable 48x1G PoE+ ports; 4x1G and 4x10G network modules for uplink ports; 2 power supply slots; 2 field-replaceab supports StackWise-160.
C9200-48T	Stackable 48x1G ports; 4x1G and 4x10G network modules for uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.

Switch Model	Description
C9200-24PXG	Stackable 8 Multigigabit Ethernet and 16x1G PoE+ ports; supports 4x10G, 2x25G and 2x40G network modules for uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-48PXG	Stackable 8 Multigigabit Ethernet and 40x1G PoE+ ports; supports 4x10G, 2x25G and 2x40G network modules for uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.
C9200-48PL	Stackable 48x1G PoE+ ports with partial PoE support; 4x1G and 4x10G network modules for uplink ports; 2 power supply slots; 2 field-replaceable fans; supports StackWise-160.

Front Panel Components

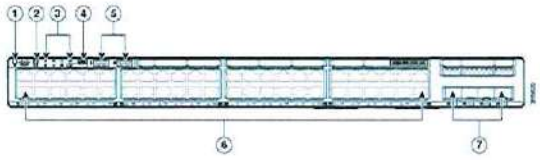
This section describes the front panel components of Cisco Catalyst 9200 Series switches :

- 24 or 48 downlink ports of one of the following types:
  - 10/100/1000
  - 10/100/1000 PoE+
- 1G/10G Uplink ports
- USB Type A storage ports
- USB mini-Type B console port
- LEDs
- Blue Beacon

All the switch models have similar components. See the following illustration for example.

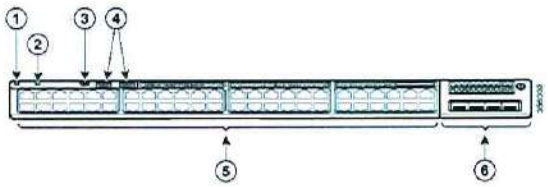
Note The Cisco Catalyst 9200 Series switches might have slight cosmetic differences on the bezels.

Figure 1: Front Panel of a C9200L Switch



1	Blue Beacon (UID button)	5	USB Type A storage ports
2	Mode button	6	10/100/1000 PoE+ ports
3	Status LEDs	7	Fixed uplink ports
4	USB mini-Type B (console) port		

Figure 2: Front Panel of a C9200 Switch



1	Blue Beacon (UID button)	4	USB Type A storage ports
2	Mode button	5	10/100/1000 PoE+ ports
3	USB mini-Type B (console) port	6	Network Module with uplink ports

10/100/1000 Ports

The 10/100/1000 ports use RJ-45 connectors with Ethernet pinouts. The maximum cable length is 328 feet (100 meters). The 100BASE-TX and 1000BASE-T traffic requires twisted pair (UTP) cable of Category 5 or higher. The 10BASE-T traffic can use Category 3 cable or higher.

PoE and PoE+ Ports

The PoE and PoE+ ports provide the following functionality:

- PoE/PoE+ ports: Support for IEEE 802.3af-compliant powered devices (up to 15.4W PoE per port) and support for IEEE 802.3at-compliant powered devices (up to 30W PoE+ per port).
- Support for pre-standard Cisco powered devices.
- Configurable support for Cisco intelligent power management, including enhanced power negotiation, power reservation, and per-port power policing.

See the Power Supply Modules, on page 9 for the power supply matrix that defines the available PoE and PoE+ power per port. The output of the PoE+ circuit has been evaluated as a Limited Power Source (LPS) per IEC 60950-1.

Multigigabit Ethernet Ports

The Multigigabit (mGig) Ethernet ports can be configured to auto-negotiate multiple speeds on switch ports. The ports support 100 Mbps, 1 Gbps, 2.5 Gbps, and 5 Gbps speeds on Category 5e (Cat5e) cables, and up to 10 Gbps over Category 6 (Cat6) and Category 6A (Cat6A) cables up to a maximum of 100 m. 10Gbps over Cat6 cable is limited for distances up to 55 m. For 10GBASE-T, Cat6a can support up to 100 m when transmitting 10Gbps. Due to the extra bandwidth requirements from the cable, additional limitations exist for best performance. These limitations include, but are not limited to cable reach, cable bundling parameters (tightness, frequency, number of cables, speed with respect to each cable) and cable termination quality.

The 802.3 channel requirements for interoperability typically limit the cable reach to 100 m, but other factors can shorten this reach. In addition, for both UPOE and HPOE and data integrity, the 100 m total should not include more than 10 m total stranded or patch cable. Therefore, it is assumed that a 100 m link includes a maximum of two 5 m patch cables of the appropriate category, and 90 m of plenum or riser (i.e. solid copper core) cables. Ensure that you follow the TIA guidance on cable dressing.

It is recommended to test the complete link using an appropriate cable tester for 10 Gbps as well as 5 Gbps links. However, even if the link passes cable testing, it is still prone to occasional errors due to aggressors in the bundle, and physical disturbances of the cables. As an example of bundling limitations, for 5 Gbps with cat5e cable, only a total 45 m bundled length is supported; the remaining 55 m should be unbundled. For bundling, follow Cisco Guidelines and Best Practices for the Installation and Maintenance of Data Networking Equipment which recommends the use of Velcro ties every 1 to 2 m for bundled sections.

If you are upgrading the network gear but reusing the existing cable plant, note that at speeds above 2.5 Gbps traditional Cat5e channel specifications do not support full 100 m reach. To ensure 5 Gbps link speeds, we recommend using Cat6a cabling. For more information, see the Whitepaper from NBASE-T alliance, which has now merged with Ethernet Alliance, archived at https://archive.nbaset.ethernetalliance.org/library/white-paper-2/.

Note Multigigabit ports do not support half duplex mode. Use full duplex mode.

Management Ports

The management ports connect the switch to a PC running Microsoft Windows or to a terminal server.

- Ethernet management port. See Ethernet Management Port, on page 12.
- RJ-45 console port (EIA/TIA-232). See RJ-45 Console Port, on page 13.
- USB mini-Type B console port (5-pin connector).

The 10/100/1000 Ethernet management port connection uses a standard RJ-45 crossover or straight-through cable. The RJ-45 console port connection uses the supplied RJ-45-to-DB-9 female cable. The USB console port connection uses a USB Type A to 5-pin mini-Type B cable. The USB console interface speeds are the same as the RJ-45 console interface speeds.

If you use the USB mini-Type B console port, the Cisco Windows USB device driver must be installed on any PC connected to the console port (for operation with Microsoft Windows). Mac OS X or Linux do not require special drivers.

The 4-pin mini-Type B connector resembles the 5-pin mini-Type B connectors. They are not compatible. Use only the 5-pin mini-Type B.

Figure 3: USB Mini-Type B Port

This illustration shows a 5-pin mini-Type B USB port.

With the Cisco Windows USB device driver, you can connect and disconnect the USB cable from the console port without affecting Windows HyperTerminal operations.

The console output always goes to both the RJ-45 and the USB console connectors, but the console input is active on only one of the console connectors at any one time. The USB console takes precedence over the RJ-45 console. When a cable is connected into the USB console port, the RJ-45 console port becomes inactive. Conversely, when the USB cable is disconnected from the USB console port, the RJ-45 port becomes active.

You can use the command-line interface (CLI) to configure an inactivity timeout which reactivates the RJ-45 console if the USB console has been activated and no input activity has occurred on the USB console for a specified time.

After the USB console deactivates due to inactivity, you cannot use the CLI to reactivate it. Disconnect and reconnect the USB cable to reactivate the USB console. For information on using the CLI to configure the USB console interface, see the Software Configuration Guide.

USB Type A Port

The USB Type A port provides access to external USB flash devices (also known as thumb drives or USB keys).

The port supports Cisco USB flash drives with capacities from 128 MB to 8 GB. USB devices with port densities of 128 MB, 256 MB, 1 GB, 4 GB, and 8 GB are supported. When combined with stacking, you can upgrade other switches in the stack from an USB key inserted in any switch within the stack. Cisco IOS software provides standard file system access to the flash device: read, write, erase, and copy, as well as the ability to format the flash device with a FAT file system.

It provides you with the ability to automatically upgrade the internal flash with the USB drive's configuration and image for emergency switch recovery using USB auto-upgrade. This feature checks the internal flash for a bootable image and configuration and if either image or the configuration is not available, then the USB drive is checked for boot images and configuration. If the boot image and configuration are available, these are copied to flash for the reboot.

Uplink Ports

The Cisco Catalyst 9200 Series switches support both fixed uplinks and modular uplinks. The C9200 switch models support modular uplinks with one hot-swappable network module that provides uplink ports to connect to other devices.

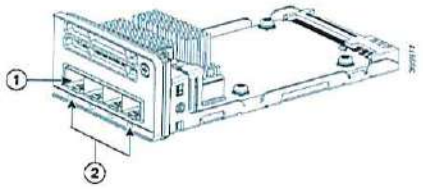
The fixed uplink ports on C9200L switch models support the following types of transceiver modules.

- 4x1G ports that support 1G SFP modules.
- 4x10G ports that support either 1G SFP or 10G SFP+ modules.
- 2x25G ports that support SFP28 modules.

For supported Cisco pluggable transceiver modules (SFP, SFP, SFP28 and QSFP+ modules), refer to the Cisco Transceiver Modules Compatibility Information at http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Note For information about installing an (uplink) transceiver module, see Installing a Cisco Pluggable Transceiver Module, on page 37.

Figure 4: Network Module C9200-NM-4G



1	Module slot	2	LEDs

The following table lists the optional Cisco Catalyst 9200 Series Switches uplink network modules with 4x1G, 4x10G, 2x25G, and 2x40G slots.

Table 3: Supported Network Modules

Network Module	Description
C9200-NM-4G	This module has four 1G SFP module slots. Any combination of standard SFP modules is supported. SFP+ modules are not supported. If you insert an SFP+ module in the 1G network module, the SFP+ module does not operate, and the switch logs an error message. This module is not supported on C9200 Multigigabit Ethernet switches.
C9200-NM-4X	This module has four 10G SFP module slots. Each port supports a 1G or 10G connection. Any combination of standard SFP modules is supported. This module is supported on both 1G and Multigigabit Ethernet switch models of C9200 switches.
C9200-NM-2Y	This module has two 25 Gigabit Ethernet SFP28 module slots. Any combination of SFP, SFP+, and SFP28 modules are supported. This module is supported only on C9200 Multigigabit Ethernet switches.

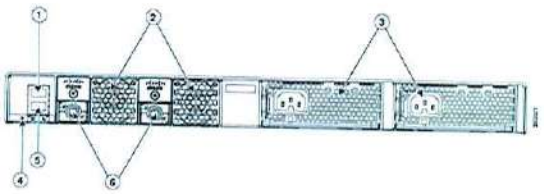
Network Module	Description
C9200-NM-2Q	This module has two 40G slots with a QSFP+ connector in each slot. This module is supported only on C9200 Multigigabit Ethernet switches.
C9200-NM-BLANK	Insert this blank module when the switch has no uplink ports to enable sufficient airflow.

Note For information about installing a network module, see Installing a Network Module, on page 34.

Rear Panel

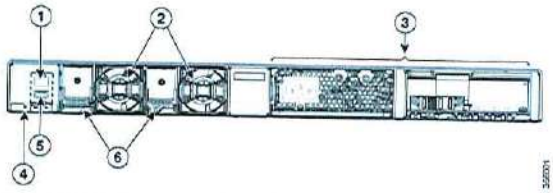
The switch rear panel includes StackWise connectors, fan modules, and power supply modules.

Figure 5: Rear Panel of a C9200L Switch



1	RJ-45 console port	4	Blue Beacon LED
2	Fixed fan modules on C9200L switches	5	MGMT (RJ-45 10/100/1000 port)
3	Power supply module slots	6	StackWise-80 port connectors

Figure 6: Rear Panel of a C9200 Switch



1	RJ-45 console port	4	Blue Beacon LED
2	Modular fan modules on C9200 switches	5	MGMT (RJ-45 10/100/1000 management port)
3	Power supply module slots	6	StackWise-160 port connector slots with stack blanks installed

RFID Tag

The switch has a built-in, front-facing, passive RFID tag that uses UHF RFID technology and requires an RFID reader with compatible software. It provides auto-identification capabilities for asset management and tracking. The RFID tags are compatible with the Generation 2 GS1 EPC Global Standard and are ISO 18000-6C compliant. They operate in the 860- to 960-MHz UHF band. For more information, see Radio Frequency Identification (RFID) on Cisco Catalyst 9000 Family Switches White Paper.

StackWise Ports

StackWise ports are used to connect switches in StackWise stacking configurations. The switch ships with a 0.5-meter StackWise cable that you can use to connect the StackWise ports. For more information on StackWise cables, see Connecting to the StackWise Ports, on page 29.

Caution Use only approved cables, and connect only to similar Cisco equipment. Equipment might be damaged if connected to nonapproved Cisco cables or equipment.

Power Supply Modules

The switch has a field replaceable main AC power supply module and a redundant hot-swappable field replaceable AC power supply module. The switch is powered through one or two internal power supply modules. In switches with PoE capability, the redundant power supply can also be used for extra PoE power.

Following are the power supply modules supported on Cisco Catalyst 9200 Series Switches:

- PWR-C5-125WAC
- PWR-C5-600WAC
- PWR-C5-1KWAC
- PWR-C6-125WAC
- PWR-C6-600WAC
- PWR-C6-1KWAC

The switch has two internal power supply module slots. You can use two AC power supply modules or one power supply module and a blank module (PWR-C5-BLANK).

The switch can operate with either one or two active power supply modules.

Switch Models, on page 1 shows the default power supply modules that ship with each switch model. All power supply modules (except the blank modules) have internal fans. All switches ship with a blank power supply module in the second power supply slot. Each AC power supply module has a power cord (CAB-TA-*XXX*) for connection to an AC power outlet.

Caution Do not operate the switch with one power supply module slot empty. For proper chassis cooling, both power supply module slots must be populated with either a power supply or a blank module.

The power supply modules are autoranging units that support input voltages between 100 and 240 VAC. The output voltage range is 12 to 12.5 V for 125W power supply and 54 to 56 V for 600W and 1000W power supplies.

All the PoE-enabled switches when installed with both the power supplies support full PoE+, 1440W on a 48-port switch and 740W on a 24-port switch.

The partial PoE-enabled switches support only 600W power supply providing a PoE budget of 370W. If the switch is installed with one power supply, the available POE budget is 370W and 740W, if there are two power supplies installed.

The following tables show the PoE available and PoE requirements for PoE switch models.

Table 4: Available PoE with AC Power Supply

Models	Default Power Supply	Available PoE	Full PoE with Redundant Power Supply
C9200 Switches			
C9200-24P	PWR-C5-600WAC or PWR-C6-600WAC	370W	740W
C9200-48P	PWR-C5-1KWAC or PWR-C6-1KWAC	740W	1440W
C9200-24T	PWR-C5-125WAC or PWR-C6-125WAC	-	-

Models	Default Power Supply	Available PoE	Full PoE with Redundant Power Supply
C9200-48T	PWR-C5-125WAC or PWR-C6-125WAC	-	-
C9200-24PB	PWR-C5-600WAC or PWR-C6-600WAC	370W	740W
C9200-48PB	PWR-C5-1KWAC or PWR-C6-1KWAC	740W	1440W
C9200-48PL	PWR-C5-600WAC or PWR-C6-600WAC	370W	740W
C9200-24PXG	PWR-C5-600WAC or PWR-C6-600WAC	370W	740W
C9200-48PXG	PWR-C5-1KWAC or PWR-C6-1KWAC	740W	1440W
C9200L Switches			
C9200L-24P-4G	PWR-C5-600WAC	370W	740W
C9200L-24P-4X	PWR-C5-600WAC	370W	740W
C9200L-24PXG-2Y	PWR-C5-600WAC	370W	740W
C9200L-24PXG-4X	PWR-C5-600WAC	370W	740W
C9200L-24T-4G	PWR-C5-125WAC	—	—
C9200L-24T-4X	PWR-C5-125WAC	—	—
C9200L-48P-4G	PWR-C5-1KWAC	740W	1440W
C9200L-48P-4X	PWR-C5-1KWAC	740W	1440W
C9200L-48PL-4G	PWR-C5-600WAC	370W	740W
C9200L-48PL-4X	PWR-C5-600WAC	370W	740W
C9200L-48PXG-2Y	PWR-C5-1KWAC	740W	1440W
C9200L-48PXG-4X	PWR-C5-1KWAC	740W	1440W
C9200L-48T-4G	PWR-C5-125WAC	—	—
C9200L-48T-4X	PWR-C5-125WAC	—	—

The power supply modules have two status LEDs.

Table 5: Switch Power Supply Module LEDs

AC OK	Description	PS OK	Description
Off	No AC input power.	Off	Output is disabled, or input is outside operating range (AC LED is off).
Green	AC input power present.	Green	Power output to switch active.
		Red	Output has failed.

Fan Modules

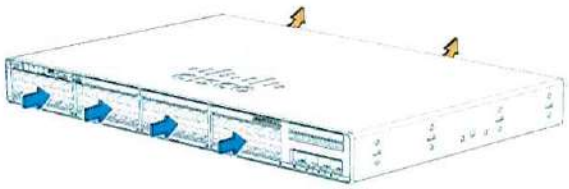
The Cisco Catalyst 9200 Series Switches supports two internal fixed 12-V fan modules and two field-replaceable fan modules (C9200-FAN=). The C9200 models support modular fans whereas the C9200L models provide two internal fixed fans.

For information about the type of fan module supported on different switch models, see Switch Models, on page 1.

The air circulation system consists of the fan modules and the power supply modules. The airflow patterns vary depending on the power supply configuration. The switch can operate at ambient temperature if one of the fans fail.

Figure 7: Switch Airflow Pattern

The following illustration shows the airflow pattern for the switches. The blue arrow shows cool airflow, and the red arrow shows warm airflow.



Ethernet Management Port

You can connect the switch to a host such as a Windows workstation or a terminal server through the 10/100/1000 Ethernet management port or one of the console ports. The 10/100/1000 Ethernet out-of-band management port is a virtual routing and forwarding (VRF) interface and uses a RJ-45 crossover or straight-through cable.

Note The 10/100/1000 Ethernet management port is an RJ-45 connector that should be connected to a Windows workstation or a terminal server. Do not connect this port to another port in the same switch or to any port within the same switch stack.

The following table shows the Ethernet management port LED colors and their meanings.

Table 6: Ethernet Management Port LED

Color	Description
Green	Link up but no activity.
Blinking green	Link up and activity.
Off	Link down.

RJ-45 Console Port

The RJ-45 console port connection uses the supplied RJ-45-to-DB-9 female cable.

The following table shows the RJ-45 console port LED colors and their meanings.

Table 7: RJ-45 Console LED

Color	Description
Green	RJ-45 console port is active.
Off	The port is not active.

Network Configurations

See the switch software configuration guide for network configuration concepts and examples of using the switch to create dedicated network segments and interconnecting the segments through Fast Ethernet and Gigabit Ethernet connections.

CHAPTER 2

Installing the Switch

Preparing for Installation

Safety Warnings

This section includes the basic installation caution and warning statements. Read this section before you start the installation procedure. Translations of the warning statements appear in the Regulatory Compliance and Safety Information guide on Cisco.com.

Warning Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals. Statement 43

Warning Do not stack the chassis on any other equipment. If the chassis falls, it can cause severe bodily injury and equipment damage. Statement 48

Warning Ethernet cables must be shielded when used in a central office environment. Statement 171

Warning Do not work on the system or connect or disconnect cables during periods of lightning activity. Statement 1001

Warning Read the installation instructions before connecting the system to the power source. Statement 1004

Warning Class 1 laser product. Statement 1008

Warning This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security. Statement 1017

Warning The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device. Statement 1019

Warning Use copper conductors only. Statement 1025

Warning This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028

Warning Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030

Warning Ultimate disposal of this product should be handled according to all national laws and regulations. Statement 1040

Warning To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: <113°F (45°C). Statement 1047

Warning Installation of the equipment must comply with local and national electrical codes. Statement 1074

Warning To prevent airflow restriction, allow clearance around the ventilation openings to be at least: 3 inches (7.6 cm). Statement 1076

Installation Guidelines

When determining where to install the switch, verify that these guidelines are met:

- Clearance to the switch front and rear panel meets these conditions:
  - Front-panel LEDs can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - AC power cord can reach from the AC power outlet to the connector on the switch rear panel.
  - The SFP/SFP+ module minimum bend radius and connector length is met. See the SFP/SFP+ module documentation for more information.
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures. Make sure that the cabling is safely away from other devices that might damage the cables.
- Make sure power-supply modules and fan modules are securely inserted in the chassis before moving the switch.
- Airflow around the switch and through the vents is unrestricted.
- For copper connections on Ethernet ports, cable lengths from the switch to connected devices can be up to 328 feet (100 meters).
- Temperature around the unit does not exceed 113°F (45°C). If the switch is installed in a closed or multirack assembly, the temperature around it might be greater than normal room temperature.
- Humidity around the switch does not exceed 95 percent.
- Altitude at the installation site is not greater than 10,000 feet.
- Cooling mechanisms, such as fans and blowers in the switch, can draw dust and other particles causing contaminant buildup inside the chassis, which can result in system malfunction. You must install this equipment in an environment as free from dust and foreign conductive material (such as metal flakes from construction activities) as is possible.

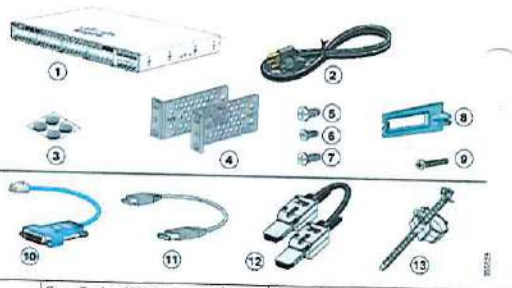
Note The illustrations used in this section shows a C9200L switch. The C9200 switch installation is similar to C9200L, follow the same steps for installing C9200 switches.

Shipping Box Contents

The shipping box contains the model of the switch you ordered and other components needed for installation. Some components are optional, depending on your order.

Note Verify that you have received these items. If any item is missing or damaged, contact your Cisco representative or reseller for instructions. Verify that you have received these items. If any item is missing or damaged, contact your Cisco representative or reseller for instructions.

Figure 2: Components delivered in the shipping box



1	Cisco Catalyst 9200 Series switch[1] (power supply modules are not displayed)	8	Cable guide
2	AC power cord	9	M4.0 x 20mm Phillips pan-head screw
3	Four rubber mounting feet	10	RJ-45 USB console cable[1]
4	Two 19-inch mounting brackets	11	(Optional) USB console cable[1]
5	4 number-12 pan-head screw	12	(Optional) StackWise cable[1] (0.5-meter, 1-meter, or 3-meter)
6	4 number-10 pan-head screws	13	Power cord retainer
7	8 number-8 Phillips flat-head screws	-	-

1. Item is orderable.

Tools and Equipment

Obtain these necessary tools:

- A Number-2 Phillips screwdriver.

Verifying Switch Operation

Before you install the switch in a rack or on a table or shelf, power on the switch and verify that it passes POST.

To power on the switch, plug one end of the AC power cord into the switch AC power connector, and plug the other end into an AC power outlet.

As the switch powers on, it begins the POST, a series of tests that runs automatically to ensure that the switch functions properly. LEDs can blink during the test. POST lasts approximately 1 minute. The SYST LED blinks green, and the other LEDs remain solid green.

When the switch completes POST successfully, the SYST LED remains green. The LEDs turn off and then reflect the switch operating status. If a switch fails POST, the SYST LED turns amber.

POST failures are usually fatal. Call Cisco technical support representative if your switch fails POST.

After a successful POST, unplug the power cord from the switch and install the switch in a rack, on a table, or on a shelf.

Planning a Switch Data Stack

Switch Stacking Guidelines

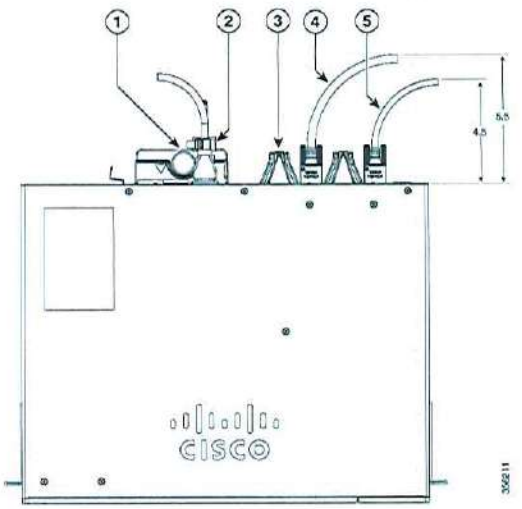
A StackWise adapter must be installed in the stacking port to enable stacking. The StackWise cable connects to the StackWise adapter in the stacking port. If the switch is not ordered with stacking, the adapters must be ordered separately and installed.

Before connecting the switches in a stack, observe these stacking guidelines:

- Number of switches in the stack. You can create data stacks with up to eight switches in a stack.
- Length of the cable. Order the appropriate cable from your Cisco sales representative. The length of the cable depends on your configuration. These are the different sizes available:
  - 0.5 meter cable (STACK-T4-50CM)
  - 1 meter cable (STACK-T4-1M)
  - 3 meter cable (STACK-T4-3M)
- Minimum bend radius and coiled diameter for StackWise cables. We recommend a minimum bend radius and coiled diameter for each StackWise cable.

Table 8: StackWise Cables Minimum Bend Radius and Coiled Diameter

Cable Part Number	Cable Length	Minimum Bend Radius	Minimum Coiled Diameter
STACK-T4-50CM	1.64 feet (0.5 m)	2.60 in. (66 mm)	5.20 in. (132 mm)
STACK-T4-1M	3.28 feet (1.0 m)	2.60 in. (66 mm)	5.20 in. (132 mm)
STACK-T4-3M	9.84 feet (3.0 m)	3.58 in. (91 mm)	7.17 in. (182 mm)



1	Power supply module	4	StackWise 3.0 m cable
2	Power cord retainer	5	StackWise 1.0 m and 0.5 m cable
3	Fan module	-	

Note Ensure that you maintain a proper clearance of 5.5 in. and 4.5 in. between the StackWise cable and the switch as depicted in the image.

Data Stack Cabling Configurations

This is an example of a recommended configuration that uses the supplied 0.5-meter StackWise cable. In this example, the switches are stacked in a vertical rack or on a table. This configuration provides redundant

connections. The configuration example uses the supplied 0.5-meter StackWise cable. The example shows the full-ring configuration that provides redundant connections.

Figure 9: Data Stacking the Switches on a Rack or on a Table Using the 0.5-meter StackWise Cables

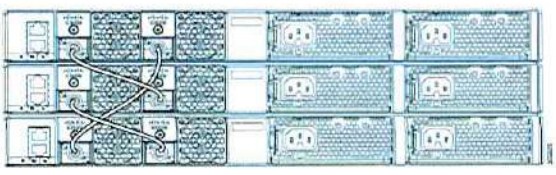
This example shows a recommended configuration when the switches are mounted side-by-side. Use the 1-meter and the 3-meter StackWise cables to connect the switches. This configuration provides redundant connections.

Figure 10: Data Stacking in a Side-by-Side Mounting

Data Stack Bandwidth and Partitioning Examples

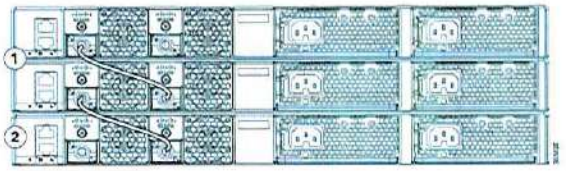
This section provides examples of data stack bandwidth and possible data stack partitioning. The figure shows a data stack of switches that provides full bandwidth and redundant StackWise cable connections.

Figure 11: Example of a Data Stack with Full Bandwidth Connections



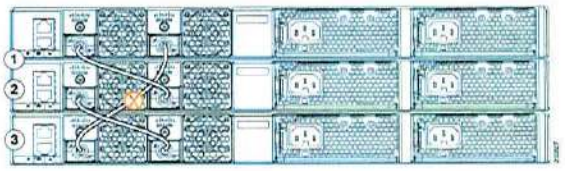
This figure shows an example of a stack of switches with incomplete StackWise cabling connections. This stack provides only half bandwidth and does not have redundant connections.

Figure 12: Example of a Data Stack with Half Bandwidth Connections



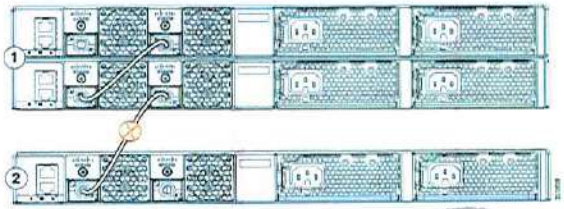
The figures below show data stacks of switches with failover conditions. In this figure, the StackWise cable is bad in link 2. Therefore, this stack provides only half bandwidth and does not have redundant connections.

Figure 13: Example of a Data Stack with a Failover Condition



In this figure, link 2 is bad. Therefore, this stack partitions into two stacks, and the top and bottom switches become the active switch in the stack. If the bottom switch is a member (not active or standby switch), it reloads.

Figure 14: Example of a Partitioned Data Stack with a Failover Condition



Power-On Sequence for Switch Stacks

Consider these guidelines before you power on the switches in a stack:

- The sequence in which the switches are first powered on might affect the switch that becomes the stack master.
- There are two ways to elect an active switch:
  - If you want a particular switch to become the active switch, configure it with the highest priority. Among switches with same priority, the switch with the lowest MAC address becomes the active switch.
  - If you want a particular switch to become the active switch, power on that switch first. This switch remains the active switch until a reelection is required. After 2 minutes, power on the other switches in the stack. If you have no preference as to which switch becomes the active switch, power on all the switches in the stack within 1 minute. These switches participate in the active switch election. Switches powered on after 2 minutes do not participate in the election.
- Power off a switch before you add it to or remove it from an existing switch stack. If changes are made to the stack without powering down the switches, the following results can occur:
  - If two operating partial ring stacks are connected together using a stack cable, a stack merge can take place. This situation reloads the whole stack (all switches in the stack).
  - If some switches in the stack are completely separated from the stack, a stack split can occur.
- A stack split can occur on a full ring stack if:
  - More than one running switch is removed without powering down.
  - More than one stack cable is removed without powering down.
- A stack split can occur in a partial ring stack if:
  - A switch is removed without powering down.
  - A stack cable is removed without powering down.
- In a split stack, depending on where the active and standby switches are located, either two stacks might be formed (with the standby taking over as the new active switch in the newly formed stack) or all the members in the newly formed stack might reload.

Note These results depend on how the switches are connected. You can remove two or more switches from the stack without splitting the stack.

For conditions that can cause a stack reelection or to manually elect the active switch, see the stacking software configuration guide *Stack Manager and High Availability Configuration Guide for Cisco Catalyst 9200 Series Switches* on Cisco.com.

Mounting the Switch

Rack-Mounting

Installation in racks other than 19-inch racks requires a bracket kit not included with the switch.

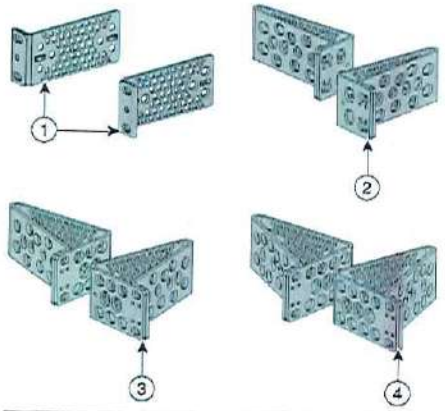
Warning To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Statement 1006

Figure 15: Rack-Mounting Brackets

This figure shows the standard 19-inch brackets and other optional mounting brackets. You can order the optional brackets (ACC-KIT-T1=) from your Cisco sales representative.



1	19-inch brackets (ACC-KIT-T1=)	3	23-inch brackets (RACK-KIT-T1=)
2	ETSI brackets (RACK-KIT-T1=)	4	24-inch brackets (RACK-KIT-T1=)

Attaching the Rack-Mount Brackets

Before you begin

You can use the minimum recommended number of two screws for installing the rack-mount bracket to each side of the switch. If required, while mounting, you can use the additional four screws provided in the accessory kit.

Procedure

Use two Phillips flat-head screws to attach the long side of the bracket to each side of the switch for the front- or rear-mounting positions.

The following illustration shows a C9200L switch. C9200 switches follow the same method for installing the rack mount bracket.

Figure 16: Attaching Brackets for 19-inch Racks in a two-post rack front-mount position

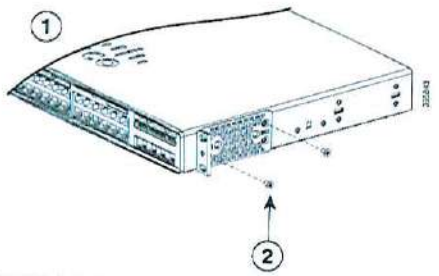
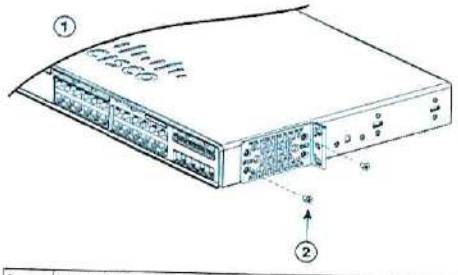


Figure 17: Attaching Brackets for 19-inch Racks in a two-post rack rear-mount position



2	Number-8 Phillips flat-head screws

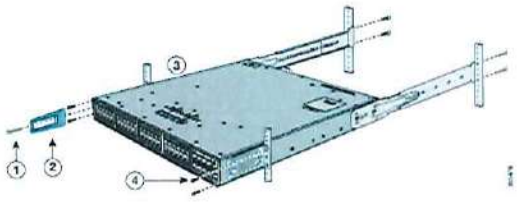
Mounting the Switch in a Rack

Procedure

Step 1 Use the four supplied Phillips machine screws to attach the brackets to the rack.

Step 2 Use the black Phillips machine screw to attach the cable guide to the left or right bracket.

Figure 18: Mounting the Switch in a Rack



1	Phillips machine screw, black	3	Front-mounting position
2	Cable guide	4	Number-12 or number-10 Phillips machine screws

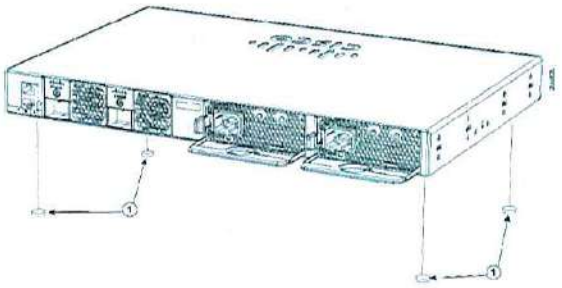
Installing the Switch on a Table or Shelf

Procedure

Step 1 To install the switch on a table or shelf, locate the adhesive strip with the rubber feet in the mounting-kit envelope.

Step 2 Attach the four rubber feet to the four circular etches on the bottom of the chassis.

Figure 19: Attaching the mounting feet for Table-Mounting or Shelf-Mounting



1	Rubber mounting feet

Step 3 Place the switch on the table or shelf near an AC power source.

What to do next

When you complete the switch installation, see After Switch Installation, on page 28 for information on switch configuration.

After Switch Installation

- Configure the switch using the Web User Interface. For more information, see "Configuring the Switch Using the Web User Interface" topic in the *Software Configuration Guide*.
- Connect the required devices to the switch ports.
- Turn on the power supply switches to power up the system. While powering up, the switch performs a series of bootup diagnostic tests.

Note The switch is designed to boot up in less than 30 minutes, provided that the neighboring devices are in fully operational state.

- Verify port connectivity after connecting devices to the switch ports. The LED turns green when the switch and the attached device have a link.

Connecting to the StackWise Ports

Before you begin

Before connecting the StackWise cables, read the "Planning a Switch Data Stack" section. Always use a Cisco-approved StackWise cable to connect the switches.

Procedure

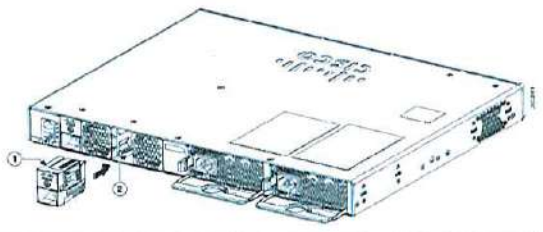
Step 1 Remove the dust covers from the StackWise cables and StackWise ports, and store them for future use.

A StackWise adapter must be installed in the StackWise port to enable stacking. In the default setup, the StackWise adapter blanks are installed in the StackWise ports. If StackWise stacking is ordered with the switch, StackWise adapters are already installed in the StackWise ports, and you can proceed to step 4.

Step 2 Remove the StackWise adapter blanks from each destination StackWise port using the Torx T15 Allen key provided in the stacking kit (or a Torx T15 screwdriver). Store them for future use.

Step 3 Install a StackWise adapter in each destination StackWise port, and secure it in place using the supplied Torx T15 key, or a Torx T15 screwdriver.

Figure 20: Installing the StackWise Adapter in a StackWise Port



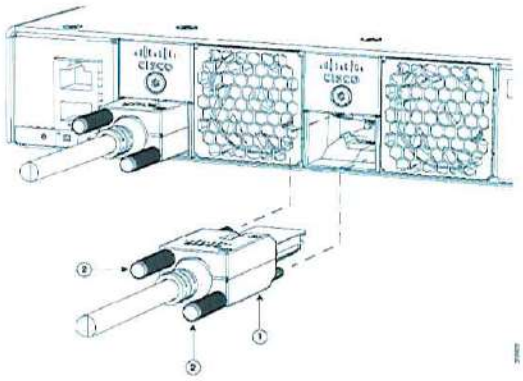
1	StackWise adapter	2	StackWise port

Step 4 Connect the cable to the StackWise port on the switch rear panel.

a) Align the StackWise cable connector with the StackWise adapter in the StackWise port.

b) Insert the StackWise cable connector into the StackWise port. Make sure that the Cisco logo is on the top side of the connector.

Figure 21: Connecting the StackWise Cable to a StackWise Port



1	Connector screws	2	StackWise cable

c) Finger-tighten the screws in clockwise direction.

Step 5 Connect the other end of the cable to the port on the other switch and finger-tighten the screws. Avoid over-tightening the screws.

Caution Removing and installing the StackWise cable can shorten its useful life. Do not remove and insert the cable more often than is absolutely necessary (installing and removing it up to 200 times is supported).

When you need to remove the StackWise cable from the connector, make sure to fully unscrew the correct screws. When the connectors are not being used, replace the dust covers.

Connecting Devices to the Ethernet Ports

10/100/1000/Multigigabit Ethernet Port Connections

The switch 10/100/1000 and Multigigabit Ethernet port configuration changes to operate at the speed of the attached device. If the attached ports do not support autonegotiation, you can manually set the speed and duplex parameters. Connecting devices that do not autonegotiate or that have the speed and duplex parameters manually set can reduce performance or result in no linkage.

To maximize performance, choose one of these methods for configuring the Ethernet ports:

- Let the ports autonegotiate both speed and duplex.
- Set the interface speed and duplex parameters on both ends of the connection.

Auto-MDIX Connections

The autonegotiation and the auto-MDIX features are enabled by default on the switch.

With autonegotiation, the switch port configurations change to operate at the speed of the attached device. If the attached device does not support autonegotiation, you can manually set the switch interface speed and duplex parameters.

With auto-MDIX, the switch detects the required cable type for copper Ethernet connections and configures the interface accordingly.

If auto-MDIX is disabled, use the guidelines in this table to select the correct cable.

Table 2: Recommended Ethernet Cables (When Auto-MDIX is Disabled)

Device	Crossover Cable	Straight-Through Cable
Switch to switch	Yes	No
Switch to hub	Yes	No
Switch to computer or server	No	Yes
Switch to router	No	Yes
Switch to IP phone	No	Yes

[1] 100BASE-TX and 1000BASE-T traffic requires twisted four-pair, Category 5 or higher. 10BASE-T traffic can use Category 3 cable or higher.

PoE and POE+ Port Connections

The 10/100/1000 PoE and PoE+ ports have the same autonegotiation settings and cabling requirements that are described in the 10/100/1000 Ports, on page 4. These ports can provide PoE and PoE+ inline power.

PoE inline power supports devices compliant with the IEEE 802.3af standard, as well as prestandard Cisco IP Phones and Cisco Aironet Access Points. Each port can deliver up to 15.4 W of PoE. PoE+ inline power supports devices compliant with the IEEE 802.3at standard, by delivering up to 30 W of PoE+ power per port to all switch ports.

See Power Supply Modules, on page 9 for the power supply modules required to support PoE and PoE+ on 24- and 48-port switches.

Warning Voltages that present a shock hazard may exist on Power over Ethernet (PoE) circuits if interconnections are made using uninsulated exposed metal contacts, conductors, or terminals. Avoid using such interconnection methods, unless the exposed metal parts are located within a restricted access location and users and service people who are authorized within the restricted access location are made aware of the hazard. A restricted access area can be accessed only through the use of a special tool, lock and key or other means of security. Statement 1072

Warning Voice over IP (VoIP) service and the emergency calling service do not function if power fails or is disrupted. After power is restored, you might have to reset or reconfigure equipment to regain access to VoIP and the emergency calling service. In the USA, this emergency number is 911. You need to be aware of the emergency number in your country. Statement 371

Caution Category 5e and Category 6 cables can store high levels of static electricity. Always ground the cables to a suitable and safe earth ground before connecting them to the switch or other devices.

Caution Noncompliant cabling or powered devices can cause a PoE port fault. Use only standard-compliant cabling to connect Cisco prestandard IP Phones and wireless access points, IEEE 802.3af, or 802.3at (PoE+)-compliant devices. You must remove any cable or device that causes a PoE fault.

CHAPTER 3

Installing a Network Module

Installing a Network Module in the Switch

Safety Warnings

This section includes the installation cautions and warnings. Translations of the safety warnings are available in the *Regulatory Compliance and Safety Information for Cisco Catalyst 9200 Series Switches* .

Read this section before you install a network module.

Caution Proper ESD protection is required whenever you handle equipment. Installation and maintenance personnel should be properly grounded by grounding straps to eliminate the risk of ESD damage to the equipment. Equipment is subject to ESD damage whenever you remove it.

Warning Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030

Warning Do not reach into a vacant slot or chassis while you install or remove a module. Exposed circuitry could constitute an energy hazard. Statement 206

Installing a Network Module

Note The switch can operate without a network module, but a blank module (with no ports or SFP slots) is available and should be installed when uplink ports are not required.

Note The switch generates logs when you insert or remove a network module with SFP/SFP+ slots.

Use only supported network modules and Cisco pluggable transceivers. Each module has an internal serial EEPROM that is encoded with security information.

The network module is hot-swappable. If you remove a module, replace it with another network module or a blank module.

Note The switch complies with EMC, safety, and thermal specifications when a network module is present. If no uplink ports are required, install a blank network module.

Before you begin

When installing network modules, observe these precautions:

- Do not remove the blank module from the slot unless you are installing a network module. A module must be in the uplink slot at all times.
- Do not remove the dust plugs from the pluggable transceivers or the rubber caps from the fiber-optic cable until you connect the cable. The plugs and caps protect the module ports and cables from contamination and ambient light.
- Removing and installing a network module can shorten its useful life. Do not remove and insert a network module more often than is necessary.
- To prevent ESD damage, follow your normal board and component handling procedures when connecting cables to the switch and other devices.

Procedure

Step 1 Attach an ESD-preventive wrist strap to your wrist and to an earth ground surface.

Step 2 Remove the module from the protective packaging.

Step 3 Remove the blank module from the switch and save it. To remove the blank module, loosen the captive screw on the module using a screwdriver until it completely disengages from the chassis.

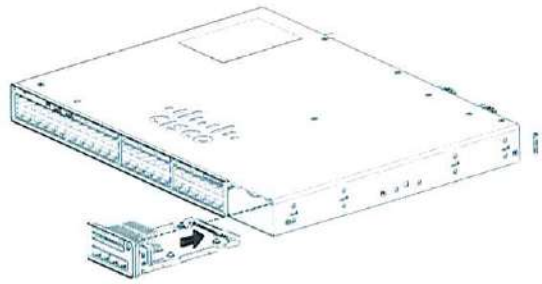
Caution Verify the correct orientation of your module before installing it. Incorrect installation can damage the module.

Caution Do not install the network module with connected cables or installed pluggable transceivers. Always remove any cables and transceiver modules before you install the network module.

Caution A module interface might become error-disabled when a network module with connected fiber-optic cables is installed or removed. If an interface is error-disabled, you can reenable the interface by using the **shutdown** and **no shutdown** interface configuration commands.

Step 4 Position the module face up to install it in the module slot. Slide the module into the slot until the screw makes contact with the chassis. Fasten the captive screws to secure the network module in place.

Figure 22: Installing the Network Module in the Switch



Removing a Network Module

Note The switch complies with EMC, safety, and thermal specifications when a network module is present. If no uplink ports are required, install a blank network module.

Note To avoid authentication failure and non-detection of modules, wait for a minimum of 6–8 seconds between the online insertion and removal (OIR) of network modules.

Procedure

Step 1 Attach an ESD-preventive wrist strap to your wrist and to an earth ground surface.

Caution Do not remove the network module with connected cables or installed pluggable transceiver modules. Always remove any cables and modules before you remove the network module.

Caution A module interface might become error-disabled when a network module with connected fiber-optic cables is installed or removed. If an interface is error-disabled, you can reenable the interface by using the **shutdown** and **no shutdown** interface configuration commands.

Step 2 Disconnect the cables from the pluggable transceiver module.

Step 3 Remove the pluggable transceiver module from the network module.

Step 4 Loosen the captive screws that hold the network module in place until it completely disengages from the chassis.

Step 5 Carefully slide the network module out of the slot.

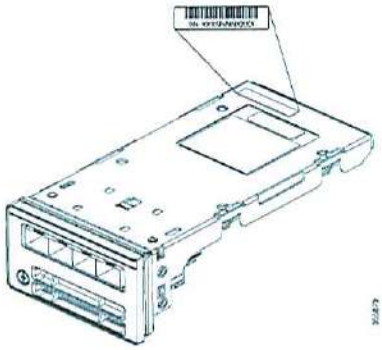
Step 6 Install a replacement network module or a blank module in the slot.

Step 7 Place the module that you removed in an antistatic bag or other protective environment.

Finding the Network Module Serial Number

If you contact Cisco Technical Assistance regarding a network module, you need to know its serial number.

Figure 23: Network Module Serial Number Location



Installing and Removing Pluggable Transceiver Modules

Installing a Cisco Pluggable Transceiver Module

Before you begin

See the switch release notes on Cisco.com for the list of supported a Cisco pluggable transceiver modules (SFP, SFP, SFP28 and QSFP+ modules). Use only supported modules on the switch. For the latest information about the supported modules, refer to the Cisco Transceiver Modules Compatibility Information.

For information about installing, removing, cabling, and troubleshooting transceiver modules, see the module documentation that shipped with your device.

Warning Class 1 laser product. Statement 1008

- Do not remove the dust plugs from the transceiver modules or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the module ports and cables from contamination and ambient light.
- Removing and installing a transceiver module can shorten its useful life. Do not remove and insert any module more often than necessary.
- To prevent ESD damage, follow your normal board and component handling procedures when connecting cables to the switch and other devices.
- When you insert several transceiver modules in multiple switch ports, wait for 5 seconds between inserting each transceiver module. This will prevent the ports from going into error disabled mode. Similarly, when you remove a transceiver module from a port, wait for 5 seconds before reinserting it.

Procedure

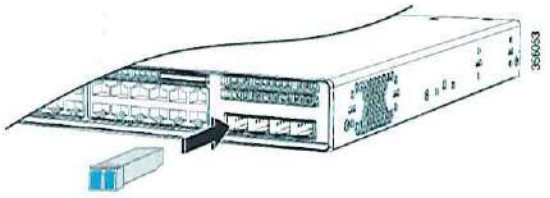
Step 1 Attach an ESD-preventive wrist strap to your wrist and to an earth ground surface.

Step 2 Find the send (TX) and receive (RX) markings that identify the top of the transceiver module.
On some transceiver modules, the send and receive (TX and RX) markings might be shown by arrows that show the direction of the connection.

Step 3 If the transceiver module has a bale-clasp latch, move it to the open, unlocked position.

Step 4 Align the module in front of the slot opening, and push until you feel the connector snap into place.

Figure 24: Installing a Transceiver Module into the Network Module

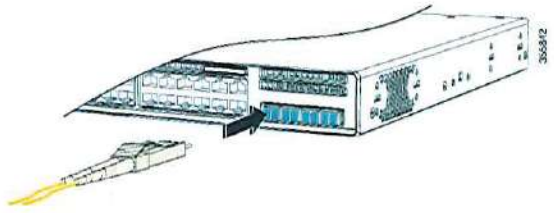


Step 5 If the module has a bale-clasp latch, close it to lock the transceiver module in place.

Step 6 Remove the transceiver module dust plugs and save.

Step 7 Connect the transceiver module cables.

Figure 25: Installing a Transceiver Module in the Uplink Module Slot



69

Removing a Cisco Pluggable Transceiver Module

Procedure

Step 1 Attach an ESD-preventive wrist strap to your wrist and to an earth ground surface.

Step 2 Disconnect the cable from the transceiver module. For reattachment, note which cable connector plug is send (TX) and which is receive (RX).

Step 3 Insert a dust plug into the optical ports of the transceiver module to keep the optical interfaces clean.

Step 4 If the module has a bale-clasp latch, pull the bale out and down to eject the module. If you cannot use your finger to open the latch, use a small, flat-blade screwdriver or other long, narrow instrument to open it.

Step 5 Grasp the transceiver module and carefully remove it from the slot.

Step 6 Place the transceiver module in an antistatic bag or other protective environment.

CHAPTER 4

Installing a Power Supply Unit

Power Supply Modules Overview

The switch chassis has two power supply slots that operates with either one active power supply module and a redundant power supply module. You can use two AC modules or one AC module and a blank cover. The active and redundant modules must be of the same type.

All power supply modules have internal fans. All switches ship with a blank cover in the second power supply slot.

The main module is field replaceable and the redundant module is hot-swappable. The redundant power supply can also be used for extra PoE power.

The following table describes the supported internal power supply modules.

Table 10: Power Supply Module Part Numbers and Descriptions

Part Number	Description
PWR-C5-125WAC	125 W AC power supply module
PWR-C5-600WAC	600 W AC power supply module
PWR-C5-1KWAC	1000 W AC power supply module
PWR-C6-125WAC[1]	125 W AC power supply module
PWR-C6-600WAC[1]	600 W AC power supply module
PWR-C6-1KWAC[1]	1000 W AC power supply module
PWR-C5-BLANK	Blank cover

1. Supported from Cisco IOS XE Gibraltar 16.11.1.

All the switches ship with a blank cover in the second power supply slot if the switches are ordered with only one power supply module.

For information about available PoE and PoE+ requirements, see these sections the Power Supply Modules, on page 9.

The power supply modules are autoranging units that support input voltages between 100 and 240 [illegible]ach AC power supply module has a power cord for connection to an AC power outlet. The modules use [illegible]VG power cord.

The following illustrations show the power supply modules.

Figure 29: 1000W AC Power Supply

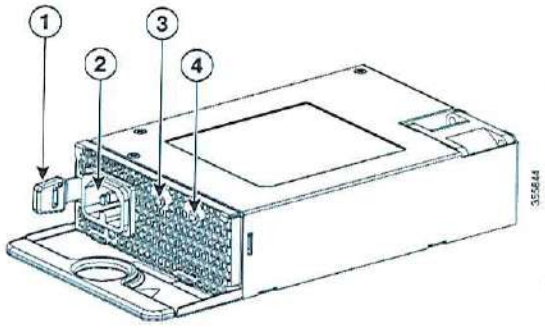
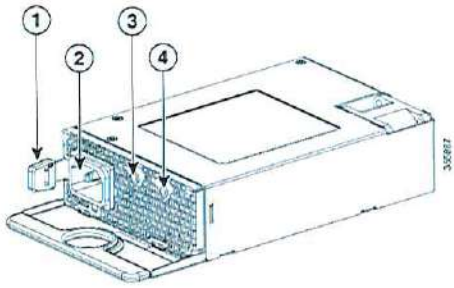


Figure 27: 125W AC Power Supply



1	Release latch	3	AC OK LED
2	AC power cord connector	4	PS OK LED

If no power supply is installed in a power supply slot, install a power supply slot cover.

Figure 28: Power Supply Slot Cover

1	Release handles	2	Retainer clips

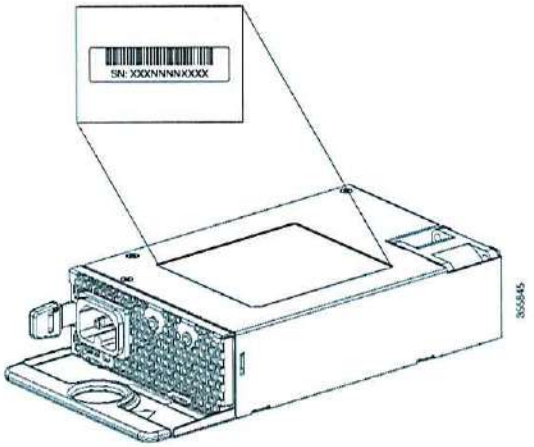
Table 11: Switch Power Supply Module LEDs

AC OK	Description	PS OK	Description
Off	No AC input power.	Off	Output is disabled, or input is outside the operating range (AC LED is off).
Green	AC input power present.	Green	Power output to switch active.
		Red	Output has failed.

Finding the Power Supply Module Serial Number

If you contact Cisco Technical Assistance regarding a power supply module, you need to know the serial number. See the following illustrations to find the serial number. You can also use the CLI to find out the serial number.

Figure 29: AC Power Supply Serial Number



Installation Guidelines

Observe these guidelines when removing or installing a power supply module.

- Do not force the power supply module into the slot. This can damage the pins on the switch if they are not aligned with the module.
- A power supply module that is only partially connected to the switch can disrupt the system operation.
- Remove power from the power supply module before removing or installing the module.
- The power supply module is hot-swappable. In some configurations, such as full PoE+ or power sharing mode, removing a power supply module causes powered devices to shut down until the power budget matches the input power of a single power supply module. To minimize network interruption, ensure that an active backup is in progress.

  For the switch commands that display available power budget, see the software configuration guide.

Caution Do not operate the switch with one power-supply module slot empty. For proper chassis cooling, both module slots must be populated, with either a power supply or a blank module.

Warning This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Statement 1024

Warning Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.

Statement 1029

Warning Do not reach into a vacant slot or chassis while you install or remove a module. Exposed circuitry could constitute an energy hazard.

Statement 206

Warning Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Statement 1030

Warning If a Cisco external power system is not connected to the switch, install the provided connector cover on the back of the switch.

Statement 386

Installing or Replacing an AC Power Supply Module

Procedure

Step 1 Turn off the power at its source.

Step 2 Remove the power cord from the power cord retainer.

Step 3 Remove the power cord from the power connector.

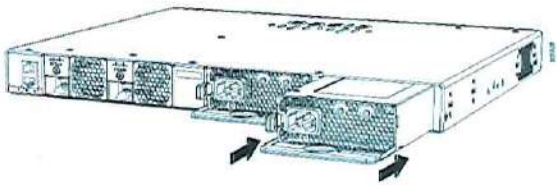
Step 4 Press the release latch at the right side of the power supply module inward and slide the power supply out.

Caution Do not leave the power-supply slot open for more than 90 seconds while the switch is operating.

Warning This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028

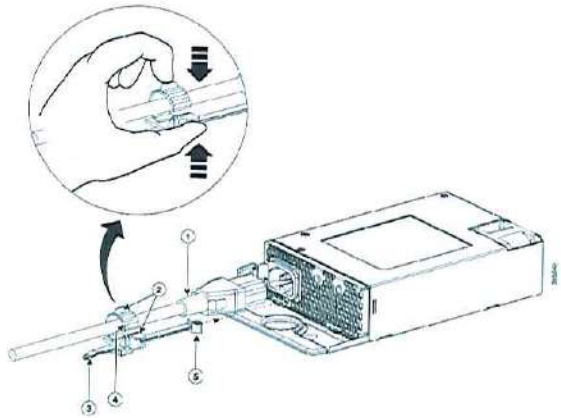
Step 5 Insert the new power supply into the power-supply slot, and gently push it into the slot. When correctly inserted, the power supplies (excluding the power cord retainer) are flush with the switch rear panel.

Figure 30: Inserting the AC-Power Supply in the Switch



Step 6 (Optional) Install the power cord retainer as follows:

Figure 31: AC-Power Supply with Power Cord Retainer



1	Power cord	4	Retainer clamp
2	Tabs on the retainer clamp	5	The strap end that is fixed to the power supply module
3	Power cord retainer strip	-	-

a) Fix the strap in the power cord retainer to the power supply module, to hold the clamp in place.
b) Slide the retainer clamp around the AC power cord and position the retainer closest to the power supply.

Note Depending on the width of the power cord, adjust the size of the retainer clamp, if required.

c) Press the tabs on the retainer clamp towards each other to secure the AC power cord.

Step 7 Connect the power cord to the power supply and to an AC power outlet. Turn on the power at the power source.

Step 8 Confirm that the power supply AC OK and PS OK LED are green.

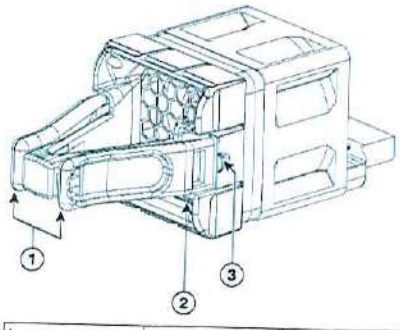
CHAPTER 5

Installing a Fan Module

Fan Modules Overview

Cisco Catalyst 9200 (C9200) Series switches support two field-replaceable fan modules providing N+1 redundancy support. The switch should be able to operate at ambient temperature if one of the fans fails.

Figure 32: Fan Module



1	Extraction handles	3	Retainer clip
2	Fan LED		

Installation Guidelines

Observe these guidelines when removing or installing a fan module:

- Do not force the fan module into the slot. This can damage the pins on the switch if they are misaligned with the module.
- A fan module that is only partially connected to the switch can disrupt the system operation.
- The switch supports hot swapping of the fan module. You can remove and replace the module without interrupting normal switch operation.

Warning Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030

Installing a Fan Module

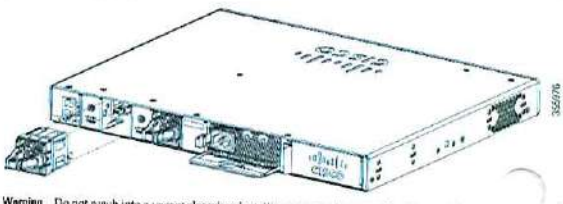
Procedure

Step 1 Pinch the fan module release handle, and slide the module out.

Caution You should replace the fan module within 5 minutes to avoid overheating the switch.

Step 2 Install the fan module in the fan slot, and firmly push it into the slot, applying pressure to the end of the module, not the extraction handles. When correctly inserted, the fan module is flush with the switch rear panel. When the fan is operating, a green LED is on in the top left corner of the fan.

Figure 33: Installing a Fan Module

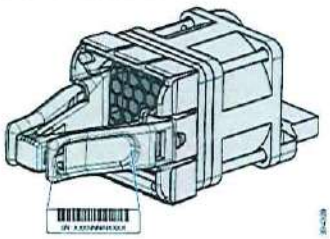


Warning Do not reach into a vacant slot when installing or removing a module. Exposed circuitry is an energy hazard. Statement 206

Finding the Fan Module Serial Number

If you contact Cisco Technical Assistance regarding a fan module, you need to know the fan module serial number. See the following illustration to find the serial number.

Figure 34: Fan Module Serial Number



CHAPTER 6

Configuring the Switch

Configuring the Switch Using the Web User Interface

For instructions on setting up the switch using the WebUI, refer to the required version of the software configuration guide. In the guide, go to *Configuring the Switch Using the Web User Interface*.

Configuring the Switch Using the CLI

Accessing the CLI Through the Console Port

You can access the CLI on a configured or unconfigured switch by connecting the RJ-45 console port or USB console port of the switch to your PC or workstation and accessing the switch through a terminal emulation program.

Note If you have stacked your switches, connect to the console port of one of the switches in the stack. You can initially configure the entire stack from any member switch.

Connecting the RJ-45 Console Port

Procedure

Step 1 Connect the RJ-45-to-DB-9 adapter cable to the 9-pin serial port on the PC. Connect the other end of the cable to the switch console port.

Step 2 Start the terminal-emulation program on the PC or the terminal. The program, frequently a PC application such as HyperTerminal or ProcommPlus, makes communication between the switch and your PC or terminal possible.

Step 3 Configure the baud rate and character format of the PC or terminal to match the console port default characteristics:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

Step 4 Power on the switch as described in the switch getting started guide.

Step 5 The PC or terminal displays the bootloader sequence. Press Enter to display the setup prompt.

Connecting the USB Console Port

Procedure

Step 1 If you are connecting the switch USB console port to a Windows-based PC for the first time, install the USB driver. See Installing the Cisco Microsoft Windows USB Device Driver, on page 55.

Note USB Type A port on the switch provides file system support and is **NOT** a console port. See USB Type A Port section.

Step 2 Connect a USB cable to the PC USB port. Connect the other end of the cable to the switch mini-B (5-pin-connector) USB console port.

Step 3 Start the terminal-emulation program on the PC or the terminal. The program, frequently a PC application such as HyperTerminal or ProcommPlus, makes communication between the switch and your PC or terminal possible.

Step 4 Configure the baud rate and character format of the PC or terminal to match the console port default characteristics:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

Step 5 Power on the switch as described in the switch getting started guide.

Step 6 The PC or terminal displays the bootloader sequence. Press Enter to display the setup prompt. Follow the steps in the Setup program.

Figure 2: Rack-Mount Brackets on Cisco 8202 Router—Port-Side Intake

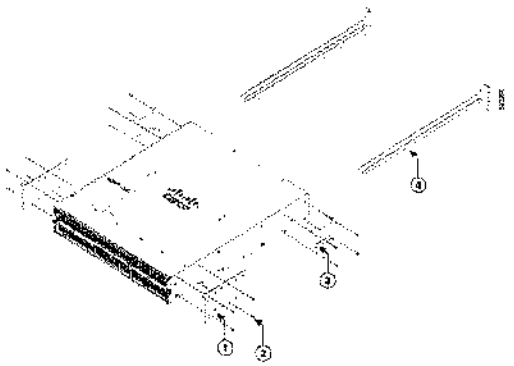
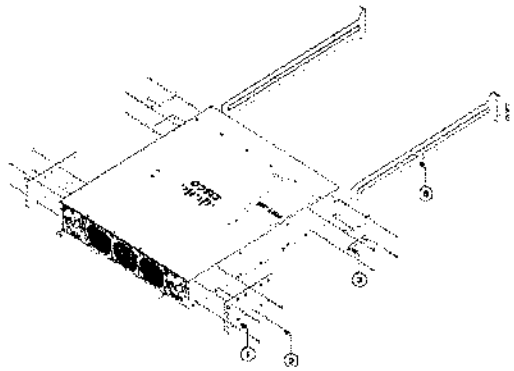


Figure 3: Rack-Mount Brackets on Cisco 8202 Router—Port-Side Exhaust



1	Rack-mount brackets	3	Rack-mount guide
2	M4 x 6mm Phillips flat-head screws	4	Rack-mount guide rails

c) Repeat Step 1b with the other rack-mount bracket on the other side of the router.

Step 2 Install the two rack-mount guides on the chassis:

a) Position a rack-mount guides on the side of the chassis with its two holes aligned to the two screw holes on the side of the chassis, and use two M4 flat-head screws to attach the guides to the chassis. Tighten the screws to a torque of 13.27 in-lb (1.5 N-m).

b) Repeat with the other rack-mount guides on the other side of the router.

Step 3 Install the guide rails to the rack:

a) Position the guide rails at the desired levels on the back side of the rack and use four 12-24 screws or four 10-32 screws, depending on the rack thread type, to attach the rails to the rack.

Note For racks with square holes, you may need to position a 12-24 cage nut behind each mounting hole in a guide rail before using a 12-24 screw.

b) Repeat with the other guide rail on the other side of the rack.

c) Use a tape measure and level to verify that the rails are at the same height and horizontal.

Step 4 Insert the router into the rack and attach:

a) Holding the router with both hands, position the back of the router between the front posts of the rack.

b) Align the two rack-mount guides on either side of the router with the guide rails installed in the rack. Slide the rack-mount guides onto the guide rails, and then gently slide the router all the way into the rack.

Note If the router does not slide easily, try realigning the rack-mount guides on the guide rails.

c) Holding the chassis level, insert two screws (12-24 or 10-32, depending on the rack type) through the holes in each of the rack-mount brackets and into the cage nuts or threaded holes in the rack-mounting rail.

d) Tighten the 10-32 screws to 20 in-lb (2.26 N-m) or tighten the 12-24 screws to 30 in-lb (3.39 N-m).

Rack-Mount the Chassis in a 2-Post Rack

This section describes how to install the Cisco 8201 or Cisco 8202 router into a cabinet or 2-p

Caution If the rack is on wheels, ensure that the brakes are engaged or that the rack is otherwise stabilized.

The following table lists the items contained in the rack-mount kit that is provided with the routers.

Table 4: Rack-Mount Kit

Quantity	Part Description
2	Rack-mount brackets
8	M4 x 0.7 x 6-mm Phillips flat-head screws

Step 1 Install two rack-mount brackets to the router:

a) Determine which end of the chassis is to be located in the cold aisle:

- If the router has port-side intake modules (fan modules and power modules with burgundy coloring), position the router so that its optical ports are in the cold aisle, and fans and power modules will be in the hot aisle.
- If the router has port-side exhaust modules (fan modules and power modules with blue coloring), position the router so that its fan and power supply modules are in the cold aisle and optical ports will be in the hot aisle.

b) With the bracket ears facing toward the center of the chassis, position a front rack-mount bracket on the side of the chassis so that the four holes are aligned to four of the screw holes on the side of the chassis.

c) Use four M4 flat-head screws with 23 in-lbs (2.6 N-m) torque value to attach the bracket to the chassis.

Figure 5: Rack-Mount Brackets on Cisco 8201 Router—Port-Side Intake

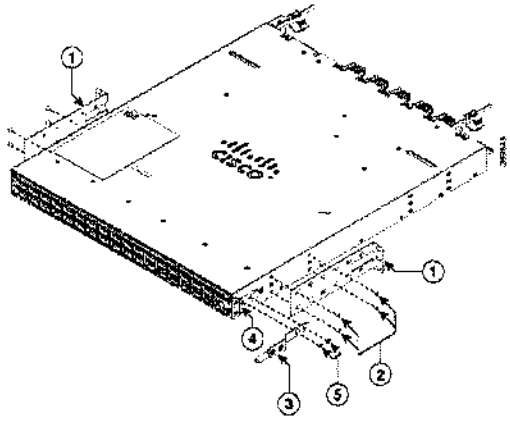
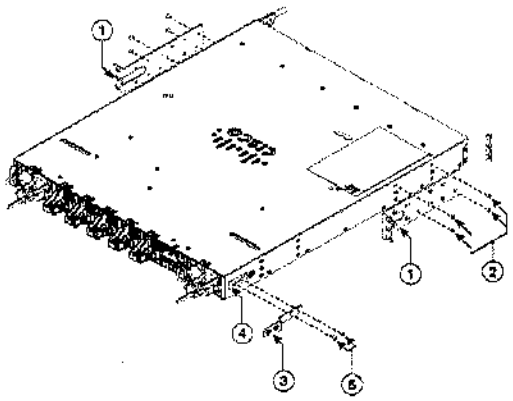


Figure 6: Figure 6 Rack-Mount Brackets on Cisco 8201 Router—Port-Side Exhaust

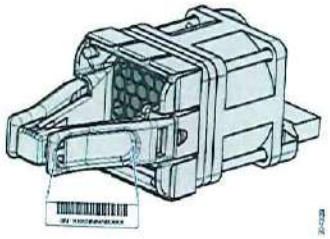


1	Rack-mount brackets	4	Remove grounding cover label
2	M4 x 6-mm Phillips flat-head screws	5	M4 x 6-mm Phillips flat-head screws
3	Grounding plate		

Finding the Fan Module Serial Number

If you contact Cisco Technical Assistance regarding a fan module, you need to know the fan module serial number. See the following illustration to find the serial number.

Figure 34: Fan Module Serial Number



CHAPTER 6

Configuring the Switch

Configuring the Switch Using the Web User Interface

For instructions on setting up the switch using the WebUI, refer to the required version of the software configuration guide. In the guide, go to *Configuring the Switch Using the Web User Interface*.

Configuring the Switch Using the CLI

Accessing the CLI Through the Console Port

You can access the CLI on a configured or unconfigured switch by connecting the RJ-45 console port or USB console port of the switch to your PC or workstation and accessing the switch through a terminal emulation program.

Note If you have stacked your switches, connect to the console port of one of the switches in the stack. You can initially configure the entire stack from any member switch.

Connecting the RJ-45 Console Port

Procedure

Step 1 Connect the RJ-45-to-DB-9 adapter cable to the 9-pin serial port on the PC. Connect the other end of the cable to the switch console port.

Step 2 Start the terminal-emulation program on the PC or the terminal. The program, frequently a PC application such as HyperTerminal or ProcommPlus, makes communication between the switch and your PC or terminal possible.

Step 3 Configure the baud rate and character format of the PC or terminal to match the console port default characteristics:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

Step 4 Power on the switch as described in the switch getting started guide.

Step 5 The PC or terminal displays the bootloader sequence. Press Enter to display the setup prompt.

Connecting the USB Console Port

Procedure

Step 1 If you are connecting the switch USB console port to a Windows-based PC for the first time, install the USB driver. See Installing the Cisco Microsoft Windows USB Device Driver, on page 55.

Note USB Type A port on the switch provides file system support and is NOT a console port. See USB Type A Port section.

Step 2 Connect a USB cable to the PC USB port. Connect the other end of the cable to the switch mini-B (5-pin-connector) USB console port.

Step 3 Start the terminal-emulation program on the PC or the terminal. The program, frequently a PC application such as HyperTerminal or ProcommPlus, makes communication between the switch and your PC or terminal possible.

Step 4 Configure the baud rate and character format of the PC or terminal to match the console port default characteristics:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

Step 5 Power on the switch as described in the switch getting started guide.

Step 6 The PC or terminal displays the bootloader sequence. Press **Enter** to display the setup prompt. Follow the steps in the Setup program.

Installing the Cisco Microsoft Windows USB Device Driver

A USB device driver must be installed the first time a Microsoft Windows-based PC is connected to the USB console port on the switch.

Installing the Cisco Microsoft Windows 7 USB Driver

Procedure

Step 1 Obtain the Cisco USB console driver file from the Cisco.com web site and unzip it.

Note You can download the driver file from the Cisco.com site for downloading the switch software.

Step 2 If using 32-bit Windows 7, double-click the setup.exe file in the Windows_32 folder. If using 64-bit Windows 7, double-click the setup(x64).exe file in the Windows_64 folder.

Step 3 The Cisco Virtual Com InstallShield Wizard begins. Click **Next**.

Step 4 The Ready to Install the Program window appears. Click **Install**.

Note If a User Account Control warning appears, click **Allow - I trust this program** to proceed.

Step 5 The InstallShield Wizard Completed window appears. Click **Finish**.

Step 6 Connect the USB cable to the PC and the switch console port. The USB console port LED turns green, and the Found New Hardware Wizard appears. Follow the instructions to complete the driver installation.

Uninstalling the Cisco Microsoft Windows USB Driver

Uninstalling the Cisco Microsoft Windows 7 USB Driver

Before you begin

Disconnect the switch console terminal before uninstalling the driver.

Procedure

Step 1 Run setup.exe for Windows 32-bit or setup(x64).exe for Windows-64-bit. Click **Next**.

Step 2 The InstallShield Wizard for Cisco Virtual Com appears. Click **Next**.

Step 3 When the Program Maintenance window appears, select the Remove radio button. Click **Next**.

Step 4 When the Remove the Program window appears, click **Remove**.

Note If a User Account Control warning appears, click **Allow - I trust this program to proceed**.

Step 5 When the InstallShield Wizard Completed window appears, click **Finish**.

APPENDIX A

Technical Specifications

Environmental and Physical Specifications

This table describes the environmental specifications.

Table 12: Environmental Specifications for the Switch

Environmental Ranges	
Operating temperature [2]	23 to 113°F (–5 to 45°C)
Storage temperature	–40 to 158°F (–40 to 70°C)
Relative humidity	5 to 90% (noncondensing)
Operating altitude	Up to 10,000 ft (3000 m)
Storage altitude	Up to 15,000 ft (4500 m)

[2] Minimum ambient temperature for cold start is 32°F (0°C)

This table describes the environmental specifications.

Table 13: Environmental Specifications for the Power Supplies

Environmental Ranges	
Operating temperature	23°F to 113°F (–5°C to 45°C) up to 5000 feet (1500m) 23°F to 104°F (–5°C to 40°C) up to 10,000 feet (3000m)
Storage temperature	–40 to 158°F (–40 to 70°C)
Relative humidity	10 to 90% (noncondensing)

Environmental Ranges	
Altitude	10,000 ft (3,000 m) up to 40°C

This table describes the physical specifications.

Table 14: Physical Specifications for the Switch

Dimensions (H x W x D)	
Chassis Dimensions	Chassis Dimensions with the FAN FRUs and the power supplies installed
1.73 x 17.5 x 13.8 in. (4.4 x 44.4 x 35 cm) C9200-24P	1.73 x 17.5 x 15.4 in. (4.4 x 44.4 x 39.1 cm) C9200-24P
1.73 x 17.5 x 13.8 in. (4.4 x 44.4 x 35 cm) C9200-24PB	1.73 x 17.5 x 15.4 in. (4.4 x 44.4 x 39.1 cm) C9200-24PB
1.73 x 17.5 x 13.8 in. (4.4 x 44.4 x 35 cm) C9200-48P	1.73 x 17.5 x 15.4 in. (4.4 x 44.4 x 39.1 cm) C9200-48P
1.73 x 17.5 x 13.8 in. (4.4 x 44.4 x 35 cm) C9200-48PB	1.73 x 17.5 x 15.4 in. (4.4 x 44.4 x 39.1 cm) C9200-48PB
1.73 x 17.5 x 13.8 in. (4.4 x 44.4 x 35 cm) C9200-48PL	1.73 x 17.5 x 15.4 in. (4.4 x 44.4 x 39.1 cm) C9200-48PL
1.73 x 17.5 x 13.8 in. (4.4 x 44.4 x 35 cm) C9200-48T	1.73 x 17.5 x 15.4 in. (4.4 x 44.4 x 39.1 cm) C9200-48T
1.73 x 17.5 x 13.8 in. (4.4 x 44.4 x 35 cm) C9200-24PXG	1.73 x 17.5 x 15.4 in. (4.4 x 44.4 x 39.1 cm) C9200-24PXG
1.73 x 17.5 x 13.8 in. (4.4 x 44.4 x 35 cm) C9200-48PXG	1.73 x 17.5 x 15.4 in. (4.4 x 44.4 x 39.1 cm) C9200-48PXG
1.73 x 17.5 x 11.3 in. (4.4 x 44.5 x 28.8 cm) C9200L-24P-4G	1.73 x 17.5 x 12.9 in. (4.4 x 44.5 x 32.9 cm) C9200L-24P-4G
1.73 x 17.5 x 11.3 in. (4.4 x 44.5 x 28.8 cm) C9200L-24P-4X	1.73 x 17.5 x 12.9 in. (4.4 x 44.5 x 32.9 cm) C9200L-24P-4X
1.73 x 17.5 x 11.3 in. (4.4 x 44.5 x 28.8 cm) C9200L-24T-4G	1.73 x 17.5 x 12.9 in. (4.4 x 44.5 x 32.9 cm) C9200L-24T-4G
1.73 x 17.5 x 11.3 in. (4.4 x 44.5 x 28.8 cm) C9200L-24T-4X	1.73 x 17.5 x 12.9 in. (4.4 x 44.5 x 32.9 cm) C9200L-24T-4X
1.73 x 17.5 x 11.3 in. (4.4 x 44.5 x 28.8 cm) C9200L-48P-4G	1.73 x 17.5 x 12.9 in. (4.4 x 44.5 x 32.9 cm) C9200L-48P-4G
1.73 x 17.5 x 11.3 in. (4.4 x 44.5 x 28.8 cm) C9200L-48P-4X	1.73 x 17.5 x 12.9 in. (4.4 x 44.5 x 32.9 cm) C9200L-48P-4X

1.73 x 17.5 x 11.3 in. (4.4 x 44.5 x 28.8 cm) C9200L-48PL-4G	1.73 x 17.5 x 12.9 in. (4.4 x 44.5 x 32.9 cm) C9200L-48PL-4G
1.73 x 17.5 x 11.3 in. (4.4 x 44.5 x 28.8 cm) C9200L-48PL-4X	1.73 x 17.5 x 12.9 in. (4.4 x 44.5 x 32.9 cm) C9200L-48PL-4X
1.73 x 17.5 x 11.3 in. (4.4 x 44.5 x 28.8 cm) C9200L-48T-4G	1.73 x 17.5 x 12.9 in. (4.4 x 44.5 x 32.9 cm) C9200L-48T-4G
1.73 x 17.5 x 11.3 in. (4.4 x 44.5 x 28.8 cm) C9200L-48T-4X	1.73 x 17.5 x 12.9 in. (4.4 x 44.5 x 32.9 cm) C9200L-48T-4X
1.73 x 17.5 x 13.8 in. (4.4 x 44.5 x 35 cm) C9200L-24PXG-4X	1.73 x 17.5 x 15.4 in. (4.4 x 44.5 x 39.1 cm) C9200L-24PXG-4X
1.73 x 17.5 x 13.8 in. (4.4 x 44.5 x 35 cm) C9200L-24PXG-2Y	1.73 x 17.5 x 15.4 in. (4.4 x 44.5 x 39.1 cm) C9200L-24PXG-2Y
1.73 x 17.5 x 13.8 in. (4.4 x 44.5 x 35 cm) C9200L-48PXG-4X	1.73 x 17.5 x 15.4 in. (4.4 x 44.5 x 39.1 cm) C9200L-48PXG-4X
1.73 x 17.5 x 13.8 in. (4.4 x 44.5 x 35 cm) C9200L-48PXG-2Y	1.73 x 17.5 x 15.4 in. (4.4 x 44.5 x 39.1 cm) C9200L-48PXG-2Y

Weight measurement is calculated with one power supply installed.

Table 15: Weight Measurements

Switch Model	Weight
C9200-24T	11 lb (5 kg)
C9200-24P	11 lb (5 kg)
C9200-24PB	11 lb (5 kg)
C9200-48T	11.5 lb (5.2 kg)
C9200-48P	11.5 lb (5.2 kg)
C9200-48PB	11.5 lb (5.2 kg)
C9200-48PL	11.5 lb (5.2 kg)
C9200-24PXG	11.4 lb (5.15 kg)
C9200-48PXG	11.9 lb (5.44 kg)
C9200L-24T-4G	9.6 lb (4.35 kg)
C9200L-24P-4G	10.4 lb (4.71 kg)
C9200L-48T-4G	10 lb (4.53 kg)
C9200L-48P-4G	10.6 lb (4.8 kg)

Switch Model	Weight
C9200L-48T-4X	10 lb (4.53 kg)
C9200L-48P-4X	10.6 lb (4.8 kg)
C9200L-24P-4X	10.4 lb (4.71 kg)
C9200L-24T-4X	9.6 lb (4.35 kg)
C9200L-48PL-4G	10.6 lb (4.8 kg)
C9200L-48PL-4X	10.6 lb (4.8 kg)
C9200L-24PXG-4X	12 lb (5.44 kg)
C9200L-24PXG-2Y	12 lb (5.44 kg)
C9200L-48PXG-4X	12.6 lb (5.71 kg)
C9200L-48PXG-2Y	12.6 lb (5.71 kg)

This table describes the physical specifications.

Table 16: Physical Specifications for the Power Supplies

Weight	
PWR-C5-125WAC	1.5 lb (0.68 kg)
PWR-C5-600WAC	1.7 lb (0.77 kg)
PWR-C5-1KWAC	2 lb (0.9 kg)
PWR-C6-125WAC	1.5 lb (0.68 kg)
PWR-C6-600WAC	1.7 lb (0.77 kg)
PWR-C6-1KWAC	2 lb (0.9 kg)
Dimensions (H x D x W) The dimensions shown include the extraction handle and the keying feature.	
PWR-C5-125WAC	1.58 x 4.0 x 7.6 in. (40.1 X 101.6 X 193 mm)
PWR-C5-600WAC	
PWR-C5-1KWAC	
PWR-C6-125WAC	
PWR-C6-600WAC	
PWR-C6-1KWAC	

Specifications for the Power Supplies and Fans

Table 17: Power Specifications for the AC Power Supplies

Power Requirements	
Maximum output power	• PWR-C5-125WAC and PWR-C6-125WAC: 125 W • PWR-C5-600WAC and PWR-C6-600WAC: 600 W • PWR-C5-1KWAC and PWR-C6-1KWAC: 1000 W
Input voltage and Frequency	100 to 240 VAC(autoranging) 50-60 Hz
Input current	• PWR-C5-125WAC and PWR-C6-125WAC: 1.6-0.7A • PWR-C5-600WAC and PWR-C6-600WAC: 7-2.8A • PWR-C5-1KWAC and PWR-C6-1KWAC: 12-6A
Output ratings	• PWR-C5-125WAC and PWR-C6-125WAC: 12V @ 10.5A • PWR-C5-600WAC and PWR-C6-600WAC: 54V @ 11.1A • PWR-C5-1KWAC and PWR-C6-1KWAC: 54V @ 16.5A
Total output BTU	• PWR-C5-125WAC and PWR-C6-125WAC: 426.5 BTUs per hour, 125W • PWR-C5-600WAC and PWR-C6-600WAC: 2047.3 BTUs per hour, 600W • PWR-C5-1KWAC and PWR-C6-1KWAC: 3412 BTUs per hour, 1000W

Table 18: Fan Module Environmental and Physical Specifications

Environmental Ranges	
Operating temperature	23 to 176°F (–5 to 80°C)
Storage temperature	–40 to 185°F (–40 to 85°C) up to 15,000 ft (4500 m)

Relative humidity	5 to 95% (noncondensing)
Altitude	Up to 13,000 ft (4000 m)
Physical Specification	
Dimensions (H x D x W)	1.62 x 1.73 x 4.24 in. (4.11 x 4.39 x 10.76 cm)
Weight (for three fans)	0.48 lb (0.21 kg)
Operating Specification	
Airflow	20 cfm

APPENDIX B

Switch LEDs

LEDs

You can use the switch LEDs to monitor switch activity and its performance.

Figure 25: Switch Front Panel LEDs

Console LED

The console LED indicates whether the USB console port or the bluetooth console is enabled.

Table 19: Console LED

LED	Color	Description
Console	Solid green	USB Mini-Type B console port is active.
	Off	USB cable not connected.

System LED

Table 20: System LED

Color	System Status
Off	System is not powered on.
Green	System is operating normally.
Blinking green	System is loading the software.
Amber	System is receiving power but is not functioning properly.
Blinking amber	There is a fault with one of the following: • Network module (non traffic-related) • Power supply • Fan module

ACTIVE LED

Table 21: ACTIVE LED

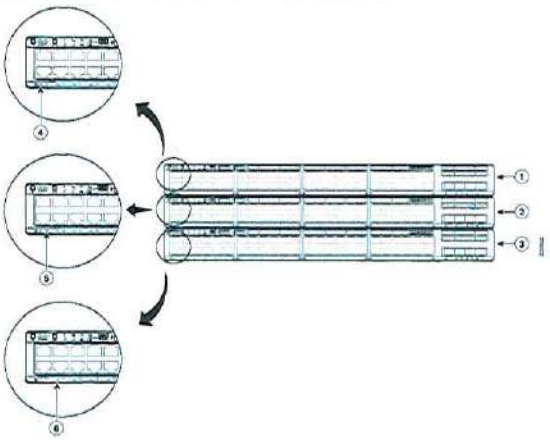
Color	Description
Off	Switch is not the active switch.
Green	Switch is the stack's active switch or a standalone switch.
Fast blinking green	Switch is in stack standby mode.
Amber	An error occurred when the switch was selecting the stack's active switch, or another type of stack error occurred.

STACK LED

The STACK LED shows the sequence of member switches in a stack. Up to eight switches can be members of a stack. The first eight port LEDs show the member number of a switch in a stack.

Figure 26: STACK LED

This figure shows the LEDs on for each switch. When you press the Mode button to select the STACK LED, the corresponding port LEDs will blink green for each switch. For example, for switch 1, port 1 will blink green and the rest of the LEDs will be off. On switch 2, port 2 will blink green and the rest of the LEDs will be off. The same behavior will be seen with the remaining switches in the stack.



1	Stack member 1	4	LED blinks green to show that this is switch 1 in the stack.
2	Stack member 2	5	LED blinks green to show that this is switch 2 in the stack.

3	Stack member 3	6	LED blinks green to show that this is switch 3 in the stack.

PoE LED

The PoE LED indicates the status of the PoE mode: either PoE or PoE+.

Table 22: PoE LED

Color	Description
Off	PoE mode is not selected. None of the 10/100/1000 ports have been denied power or are in a fault condition.
Green	PoE mode is selected, and the port LEDs show the PoE mode status.
Blinking amber	PoE mode is not selected. At least one of the 10/100/1000 ports has been denied power, or at least one of the 10/100/1000 ports has a PoE mode fault.

Port LEDs and Modes

Each Ethernet port, 1-Gigabit Ethernet module slot, and 10-Gigabit Ethernet module slot has a port LED. These port LEDs, as a group or individually, display information about the switch and about the individual ports. The port mode determines the type of information shown by the port LEDs.

To select or change a mode, press the Mode button until the desired mode is highlighted. When you change port modes, the meanings of the port LED colors also change.

When you press the Mode button on any switch in the switch stack, all the stack switches change to show the same selected mode. For example, if you press the Mode button on the active switch to show the SPEED LED, all the other switches in the stack also show the SPEED LED.

Table 23: Port Mode LEDs

Mode LED	Port Mode	Description
STAT	Port status	The port status. This is the default mode.
SPEED	Port speed	The port operating speed: 10, 100, or 1000 Mb/s.
DUPLX	Port duplex mode	The port duplex mode: full duplex or half duplex.
ACTV	Active	The active switch status.
STACK	Stack member status StackWise port status	Stack member status. The StackWise port status. See STACK LED, on page 65.
PoE[2]	The PoE+ port status.	The PoE+ port status.

[3] Only switches with PoE+ ports.

Table 24: Meaning of Switch LED Colors in Different Modes

Port Mode	Port LED Color	Meaning
STAT (port status)	Off	No link, or port was administratively shut down.
	Green	Link present, no activity.
	Blinking green	Activity. Port is sending or receiving data.
	Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
	Amber	Port is blocked by Spanning Tree Protocol (STP) and is not forwarding data. After a port is reconfigured, the port LED can be amber for up to 30 seconds as STP checks the switch for possible loops.
SPEED	**10/100/1000/SFP ports**	
	Off	Port is operating at 10 Mb/s.
	Green	Port is operating at 100 Mb/s.
	Single green flash (on for 100 ms, off for 1900 ms)	Port is operating at 1000 Mb/s.
	Uplink ports	
	Off	Port is not operating.
	Blinking green	Port is operating at up to 10 Gb/s.
DUPLX (duplex)	Off	Port is operating in half duplex.
	Green	Port is operating in full duplex.
ACTV (data active switch)	Off	The switch is not the active switch. **Note** For a standalone switch, this LED is off.
	Green	The switch is the active switch.
	Amber	Error during active switch election.
	Blinking green	Switch is a standby member of a data stack and assumes active responsibilities if the current active switch fails.

Port Mode	Port LED Color	Meaning
STACK (stack member)	Off	No stack member corresponding to that member number.
	Blinking green	Stack member number.
	Green	Member numbers of other stack member switches.
PoE[4]	Off	PoE+ is off. If the powered device is receiving power from an AC power source, the port LED is off even if the device is connected to the switch port.
	Green	PoE+ is on. The port LED is green when the switch port is providing power.
	Alternating green-amber	PoE+ is denied because providing power to the powered device will exceed the switch power capacity.
	Blinking amber	PoE+ is off due to a fault or because it has exceeded a limit set in the switch software. **Caution** PoE+ faults occur when noncompliant cabling or powered devices are connected to a PoE+ port. Use only standard-compliant cabling to connect Cisco prestandard IP Phones and wireless access points or IEEE 802.3af-compliant devices to PoE+ ports. You must remove from the network any cable or device that causes a PoE+ fault.
	Amber	PoE+ for the port has been disabled. **Note** PoE+ is enabled by default

[4] Only switches with PoE or PoE+ ports.

Beacon LED

The UID and the Beacon LED can be turned on by the administrator to indicate that the switch needs attention. It helps the administrator identify the switch. The beacon can be turned on by either pressing the UID button on the switch front panel, or by using the CLI. There is a blue beacon on the front and rear panel of the switch. The blue beacon on the front panel is a button labeled UID, and on the back panel it is a LED labeled BEACON.

Color/State	Description
Solid blue	The operator has indicated that the system needs attention.

RJ-45 Console Port LED

Table 25: RJ-45 Console Port LED

Color	RJ-45 Console Port Status
Off	RJ-45 console is disabled. USB console is active.
Green	RJ-45 console is enabled. USB console is disabled.

Fan LED

Table 26: Fan LED Indicator

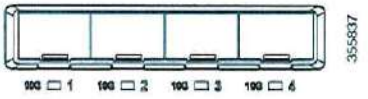
Color/State	Description
Off	The fan is not receiving power; the fans have stopped.
Green	All fans are operating normally.
Amber	One or more fans have encountered tachometer faults.
Red	One or more fans' tachometer faults have exceeded the maximum limit.

Uplink Port LEDs

The uplink ports have various status LEDs. Each port LED is labeled according to its module status.

- For SFP ports, a G labeling nomenclature is used, where G = 1 Gigabit. The The G label appears to the left of the uplink port LED.
- For SFP+ ports, a 10G labeling nomenclature is used, where 10G = 10 Gigabit. The 10G label appears to the left of the uplink port LED. SFP+ module ports support both SFP+ and SFP modules
- For SFP28 ports, a 25G labeling nomenclature is used, where 25G = 25 Gigabit. The The G label appears to the left of the uplink port LED.
- For QSFP+ ports, a 40G labeling nomenclature is used, where 40G = 40 Gigabit. The The G label appears to the left of the uplink port LED.

Figure 32: SFP+ Port LEDs



Color	Network Module Link Status
Off	Link is off.
Green	Link is on; no activity.
Blinking green	Activity on a link; no faults. **Note** The LED will blink green even when there is very little control traffic.
Blinking amber	Link is off due to a fault or because it has exceeded a limit set in the switch software. **Caution** Link faults occur when non-compliant cabling is connected to an SFP/SFP+ port. Use only standard-compliant cabling to connect to Cisco SFP/SFP+ ports. You must remove from the network any cable or device that causes a link fault.
Amber	Link for the SFP/SFP+/SFP28/QSFP+ has been disabled.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR ANY RENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content or examples is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Hardware Installation Guide for Cisco 8200 Series Routers

First Published: 2020-08-15
Last Modified: 2020-09-03

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Cisco 8200 Series Routers Overview

Cisco 8200 Series Routers

The Cisco 8200 Series Routers utilizes Cisco's new Router-on-Chip (RoC) model to deliver full routing functionality with a single ASIC per router. The RoC architecture is distinguished from System-on-Chip (SoC) switches by supporting large forwarding tables, deep buffers, more flexible packet operations, and enhanced programmability.

The Cisco 8200 series routers presently comprises:

- Cisco 8201 Router – It provides 10.8 Tbps of network bandwidth with dramatically lower power consumption than contemporary 10 Tbps systems. The Cisco 8201 Router is a fixed port, high density, one rack unit form-factor router. Supported ports include 24x 400G QSFP-DD and 12x 100G QSFP28. For more details on ports and supported breakout options, see "Interfaces and Port Description, on page 34".
- Cisco 8202 Router – It provides 10.8 Tbps of network bandwidth with dramatically lower power consumption than contemporary 10 Tbps systems. The Cisco 8202 Router is a fixed port, high density, two rack unit form-factor router. Supported ports include 12x400 GbE QSFP-DD and 60x100 GbE QSFP28. For more details on ports and supported breakout options, see "Interfaces and Port Description, on page 34".

CHAPTER 2

Prepare for Installation

Note The images in this chapter are only for representational purposes, unless specified otherwise. The chassis' actual appearance and size may vary.

Warning **Statement 1071**—Warning Definition

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry, and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Safety Guidelines

Before you perform any procedure in this document, review the safety guidelines in this section to avoid injuring yourself or damaging the equipment. The following guidelines are for your safety and to protect the equipment. Because the guidelines do not include all hazards, be constantly alert.

- Keep the work area clear, smoke and dust-free during and after installation. Do not allow dirt or debris to enter into any laser-based components.
- Do not wear loose clothing, jewelry, or other items that could get caught in the router or other associated components.
- Cisco equipment operates safely when used in accordance with its specifications and prodi instructions.
- If potentially hazardous conditions exist, do not work alone.
- Take care when connecting multiple units to the supply circuit so that wiring is not overloaded.
- This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain about whether suitable grounding is available.
- When installing or replacing the unit, the ground connection must always be made first and disconnected last.
- To prevent personal injury or damage to the chassis, never attempt to lift or tilt the chassis using the handles on modules (such as power supplies, fans, or cards); these types of handles are not designed to support the weight of the unit.
- Hazardous voltage or energy is present on the backplane when the system is operating. Use caution when servicing.

Compliance and Safety Information

The Cisco 8000 Series Routers are designed to meet the regulatory compliance and safety approval requirements. For detailed safety information, see *Regulatory Compliance and Safety Information—Cisco 8000 Series Routers*.

Laser Safety

Warning **Statement 1051**—Laser Radiation

Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

Warning **Statement 1055**—Class 1/1M Laser

Invisible laser radiation is present. Do not expose to users of telescopic optics. This applies to Class 1/1M laser products.

Warning **Statement 1255**—Laser Compliance Statement

Pluggable optical modules comply with IEC 60825-1 Ed. 3 and 21 CFR 1040.10 and 1040.11 with or without exception for conformance with IEC 60825-1 Ed. 3 as described in Laser Notice No. 56, dated May 8, 2019.

Energy Hazard

The routers can be configured for a DC power source. Do not touch terminals while they are live. Observe the following warning to prevent injury.

Warning **Statement 1086**—Power Terminals

Hazardous voltage or energy may be present on power terminals. Always replace cover when terminals are not in service. Be sure uninsulated conductors are not accessible when cover is in place.

Preventing Electrostatic Discharge Damage

Many router components can be damaged by static electricity. Not exercising the proper electrostatic discharge (ESD) precautions can result in intermittent or complete component failures. To minimize the potential for ESD damage, always use an ESD-preventive antistatic wrist strap (or ankle strap) and ensure that it makes adequate skin contact.

Note Check the resistance value of the ESD-preventive strap periodically. The measurement should be 1–10 megohms.

Before you perform any of the procedures in this guide, attach an ESD-preventive strap to your wrist and connect the leash to the chassis.

Cautions and Regulatory Compliance Statements for NEBS

The NEBS-GR-1089-CORE regulatory compliance statements and requirements are discussed in this section.

Warning The intrabuilding port(s) of the equipment or subassembly, which is the management Ethernet port, must use shielded intrabuilding cabling/wiring that is grounded at both ends. Statement 7003

Warning The intrabuilding port(s) of the equipment or subassembly, which is the management Ethernet port, must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intrabuilding interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring. Statement 7005

Warning This equipment shall be connected to AC mains provided with a surge protective device (SPD) at the service equipment complying with NFPA 70, the National Electrical Code (NEC). Statement 7012

Warning This equipment is suitable for installations utilizing the Common Bonding Network (CBN). Statement 7013

Warning The battery return conductor of this equipment shall be treated as (DC-I). Statement 7016

Warning This equipment is suitable for installation in Network Telecommunications Facilities. Statement 8015

Warning This equipment is suitable for installation in locations where the NEC applies. Statement 8016

Installation Guidelines

Before installing the chassis, ensure that the following guidelines are met:

- Site is properly prepared so that there is sufficient room for installation and maintenance.
- Operating environment is within the ranges that are listed in Environment and Physical specifications.
- Chassis is mounted at the bottom of the rack if it is the only unit in the rack.

- When mounting the chassis in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the chassis in the rack.
- Airflow around the chassis and through the vents is unrestricted.
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures. Make sure that the cabling is safely away from other devices that might damage the cables.
- Each port must match the wave-length specifications on each end of the cable, and the cable must not exceed the stipulated cable length.

Note Cisco 8000 Series Routers function in operating temperatures of up to 40°C at sea level. For every 300 meters (1000 ft) elevation upto 1800 meters (6000 ft), the maximum temperature is reduced by 1°C. For more details on environmental requirements, see Cisco 8000 Series Routers Data Sheet.

Note When the Cisco 8200 Series Routers use port side exhaust fans and power supplies, the maximum temperature is reduced by 5°C (for example, 35°C at sea level or 30°C at 1500 meters).

Procure Tools and Equipment

Obtain these necessary tools and equipment for installing the chassis:

- Number 1 and number 2 Phillips screwdrivers with torque capability to rack-mount the chassis.
- 3/16-inch flat-blade screwdriver.
- Tape measure and level.
- ESD wrist strap or other grounding device.
- Antistatic mat or antistatic foam.
- Two-hole ground lug (1).
- Pair of mounting guide rails.
- Grounding cable sized according to local and national installation requirements; the required length depends on the proximity of the switch to proper grounding facilities. Cisco provides a 6 AWG lug.
- A crimping tool specified by the lug manufacturer that is large enough to accommodate the girth of the lug.
- Wire-stripping tool.
- M4 screws to fix brackets (16).
- M4 screws to fix a ground lug (2).

Accessory Kit

The following table contains the accessory kit PID and the items present in the accessory kit of the routers. The rack mount kit present in the accessory kit contains the screws and brackets required for installation.

Router	Accessory Kit-1	Items in Accessory Kit -1
Cisco 8201 Router	8200-1RU-KIT	Rack mount kit and ground lug kit
Cisco 8202 Router	8200-2RU-KIT	Rack mount kit and ground lug kit

Air filters are available only for Cisco 8202 chassis. The port side intake air filter (8202-FILTER-PI) is preinstalled on the Cisco 8202 chassis. For port side exhaust configuration, you must order the FILTER-2RU-PE air filter.

Note Air filters are for single time use only.

The following table contains the air filter accessory kit PID and the items description:

Table 1: Cisco 8202 Router Air Filter

Router	Air Filter Accessory Kit	Description
Cisco 8202 Router	8202-FILTER-PI	Port side air filter assembly for Port-Side-Intake configuration.
Cisco 8202 Router	FILTER-2RU-PE	Fan side air filter assembly for Port-Side-Exhaust configuration.

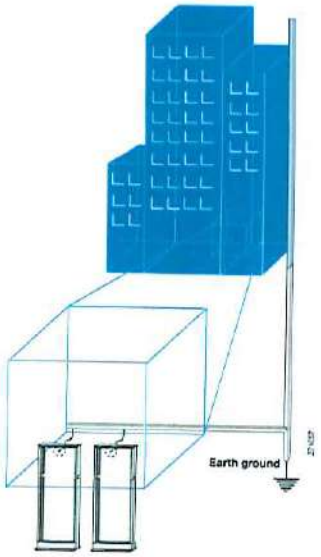
Prepare Your Location

This section illustrates how the building that houses the chassis must be properly grounded to the earth ground.

Note Unless specified otherwise, the image is only for representational purposes. The rack's actual appearance and size may vary.

Note This image is only for representational purposes. Your grounding requirement depends on your building.

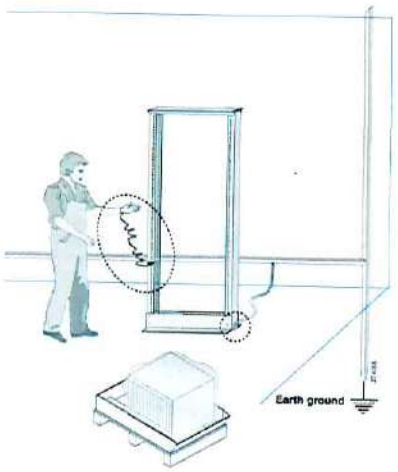
Figure 1: Building with Rack Room Connected to Earth Ground



Prepare Yourself

This section illustrates how to prepare yourself before removing the chassis from the sealed antistatic bag. The figures show how to cuff the ESD strap around the wrist and the ground cord that connects the cuff to the ground. ESD wrist straps are the primary means of controlling static charge on personnel.

Figure 2: Wearing the ESD Strap



Prepare Rack for Chassis Installation

Install the Cisco 8200 Series Routers on a standard 19 inch, Electronic Industries Alliance (EIA) with mounting rails that conform to English universal hole spacing according to Section 1 of the ANSI/EIA-310-D-1992 standard.

Note The Cisco 8201, Cisco 8202 router rack mount kit contains the rack mounting brackets for 19-inch rack. To install the chassis in a 23-inch rack or an ETSI rack, you need adapter plates to accommodate the 19-inch rack mount brackets.

The spacing between the posts of the rack must be (EIA-310-D-1992 19-inch rack compatible) wide enough to accommodate the width of the chassis.

Figure 3: Rack Specification EIA (19 and 23 inches)

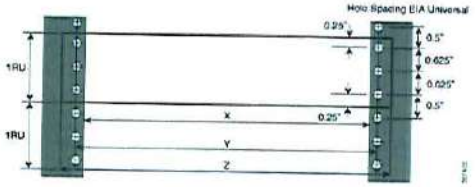


Table 2: Rack Specification EIA (19 and 23 inches)

Post Type	Rack Type	Rack Front Opening (X)	Rack Mounting Hole Center-Center (Y)	Mounting Flange Dimension (Z)
4 Post	19 inches (48.3 centimeters)	450.8mm (17.75")	465mm (18.312")	482.6mm (19")
2 Post				
4 Post	23 inches (58.4 centimeters)	552.45mm (21.75")	566.7mm (22.312")	584.2mm (23")
2 Post				

Before you move the chassis or mount the chassis into the rack, we recommend that you do the following:

Step 1 Place the rack at the location where you plan to install the chassis.

Step 2 (Optional) Secure the rack to the floor.

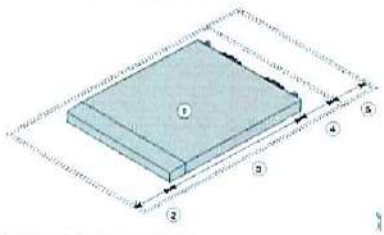
To bolt the rack to the floor, a floor bolt kit (also called an anchor embedment kit) is required. For information on bolting the rack to the floor, consult a company that specializes in floor mounting kits (such as Hilti; see Hilti.com for details). Make sure that floor mounting bolts are accessible, especially if annual retorquing of bolts is required.

Note Ensure that the rack in which the chassis is being installed is grounded to earth ground.

Clearance Requirements

The chassis requires front-to-back airflow. Leave at least 6.0 in. (15.24 cm) front and rear clearance for air intake or exhaust. We recommend that you have at least 6.0 in. (15.24 cm) of space in front of the chassis to provide room to maneuver the cables to make the required connections. Leave an extra 6.0 in. (15.24 cm) rear clearance for removal and installation of power supplies and fan modules.

Figure 4: Clearances Required Around the Chassis



1	Chassis	4	6.0 in. (15.24 cm) rear clearance for air intake/exhaust.
2	6.0 in. (15.24 cm) front clearance for air intake/exhaust.	5	More 6.0 in. (15.24 cm) rear clearance for removal and installation of power supplies and fan modules.
3	20.01 in. (50.82 cm) Chassis depth.		

CHAPTER 3

Installing the Chassis

Rack Mount the Chassis

The chassis can be mounted on a 4-post or a 2-post rack.

- Rack-Mount the Chassis in a 4-Post Rack , on page 13 - Contains the procedures for mounting the chassis in a 4-post rack.
- Rack-Mount the Chassis in a 2-Post Rack, on page 18 - Contains procedures for mounting the chassis in a 2-post rack.

Rack-Mount the Chassis in a 4-Post Rack

This section describes how to install the router in a 4-post rack.

⚠

Caution If the rack is on wheels, ensure that the brakes are engaged or that the rack is otherwise stabilized.

The following table lists the items that are contained in the rack-mount kit.

Table 2: Rack-Mount Kit

Quantity	Part Description
2	Rack-mount brackets
18	M4 x 6-mm Phillips flat-head screws
2	M4 x 6-mm Phillips pan-head screws

Quantity	Part Description
2	Rack-mount guides
2	Rack-mount guide rails, 2 lengths for different 4-post depths
(only Cisco 8201) 1	(only Cisco 8201) Grounding plate
1	Grounding lug and screws

Step 1 Install the rack-mount brackets to the router as follows:

a) Determine which end of the chassis is to be located in the cold aisle as follows:

- If the router has port-side intake modules (fan modules and power modules with burgundy coloring), position the router so that the ports are in the cold aisle.
- If the router has port-side exhaust modules (fan modules and power modules with blue coloring), position the router so that the fan and power supply modules are in the cold aisle.

b) Position a rack-mount bracket on the side of the chassis with its four holes that are aligned to four of the screw holes on the side of the chassis, and then use four M4 flat-head screws with 23 in-lbs (2.6 N-m) torque value to attach the bracket to the chassis.

Note (Only 8201) Remove the grounding cover label and align the grounding plate with the grounding holes in the chassis and attach the rack mount brackets.

Note You can align four holes in the rack-mount bracket to four screw holes on the front side of chassis or four screw holes on the rear side of the chassis. The holes that you use depend on which end of your chassis is located in the cold aisle.

Figure 5: Rack-Mount Brackets on Cisco 8201 Router—Port-Side Intake

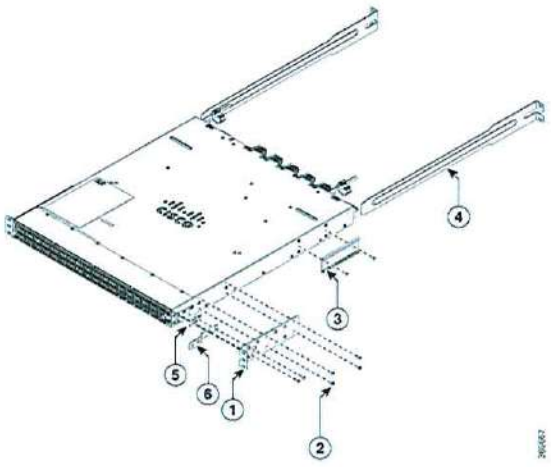
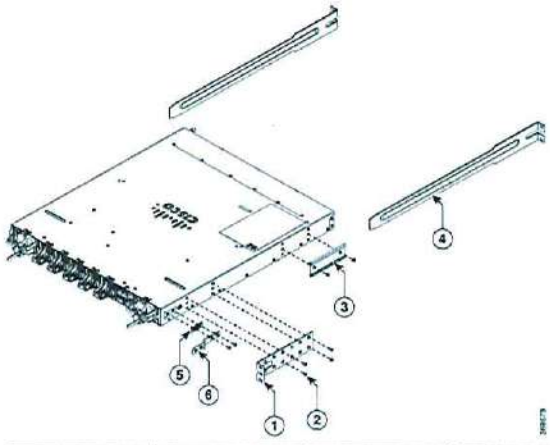


Figure 6: Rack-Mount Brackets on Cisco 8201 Router—Port-Side Exhaust



1	Rack-mount brackets	4	Rack-mount guide rails
2	M4 x 6mm Phillips flat-head screws	5	Remove grounding cover label
3	Rack-mount guide	6	Grounding plate

Figure 7: Rack-Mount Brackets on Cisco 8202 Router—Port-Side Intake

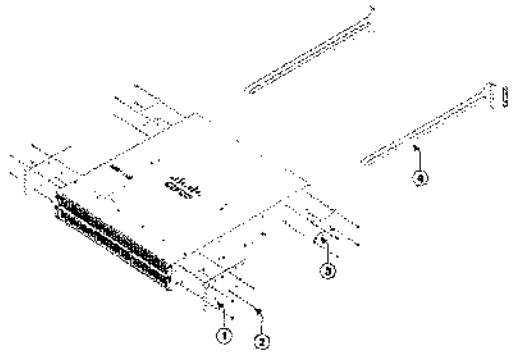
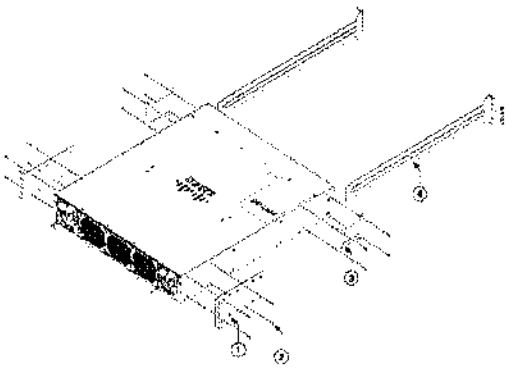


Figure 8: Rack-Mount Brackets on Cisco 8202 Router—Port-Side Exhaust



1	Rack-mount brackets	3	Rack-mount guide
2	M4 x 6mm Phillips flat-head screws	4	Rack-mount guide rails

c) Repeat Step 1b with the other rack-mount bracket on the other side of the router.

Step 2 Install the two rack-mount guides on the chassis:

a) Position a rack-mount guides on the side of the chassis with its two holes aligned to the two screw holes on the side of the chassis, and use two M4 flat-head screws to attach the guides to the chassis. Tighten the screws to a torque of 13.27 in-lb (1.5 N-m).

b) Repeat with the other rack-mount guides on the other side of the router.

Step 3 Install the guide rails to the rack:

a) Position the guide rails at the desired levels on the back side of the rack and use four 12-24 screws or four 10-32 screws, depending on the rack thread type, to attach the rails to the rack.

Note For racks with square holes, you may need to position a 12-24 cage nut behind each mounting hole in a guide rail before using a 12-24 screw.

b) Repeat with the other guide rail on the other side of the rack.

c) Use a tape measure and level to verify that the rails are at the same height and horizontal.

Step 4 Insert the router into the rack and attach:

a) Holding the router with both hands, position the back of the router between the front posts of the rack.

b) Align the two rack-mount guides on either side of the router with the guide rails installed in the rack. Slide the rack-mount guides onto the guide rails, and then gently slide the router all the way into the rack.

Note If the router does not slide easily, try realigning the rack-mount guides on the guide rails

c) Holding the chassis level, insert two screws (12-24 or 10-32, depending on the rack type) through the holes in ends of the rack-mount brackets and into the cage nuts or threaded holes in the rack-mounting rail.

d) Tighten the 10-32 screws to 20 in-lb (2.26 N-m) or tighten the 12-24 screws to 30 in-lb (3.39 N-m).

Rack-Mount the Chassis in a 2-Post Rack

This section describes how to install the Cisco 8201 or Cisco 8202 router into a cabinet or 2-po

⚠

Caution If the rack is on wheels, ensure that the brakes are engaged or that the rack is otherwise stabilized.

The following table lists the items contained in the rack-mount kit that is provided with the routers.

Table 4: Rack-Mount Kit

Quantity	Part Description
2	Rack-mount brackets
8	M4 x 0.7 x 6-mm Phillips flat-head screws

Step 1 Install two rack-mount brackets to the router:

a) Determine which end of the chassis is to be located in the cold aisle.

- If the router has port-side intake modules (fan modules and power modules with burgundy coloring), position the router so that its optical ports are in the cold aisle, and fans and power modules will be in the hot aisle.
- If the router has port-side exhaust modules (fan modules and power modules with blue coloring), position the router so that its fan and power supply modules are in the cold aisle and optical ports will be in the hot aisle.

b) With the brackets ears facing toward the center of the chassis, position a front rack-mount bracket on the side of the chassis so that the four holes are aligned to four of the screw holes on the side of the chassis.

c) Use four M4 flat-head screws with 23 in-lbs (2.6 N-m) torque value to attach the bracket to the chassis.

Figure 9: Rack-Mount Brackets on Cisco 8201 Router—Port-Side Intake

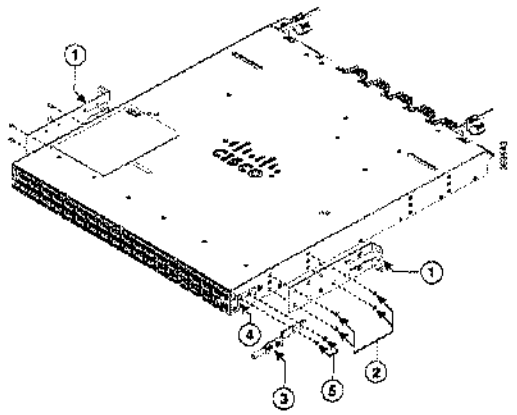
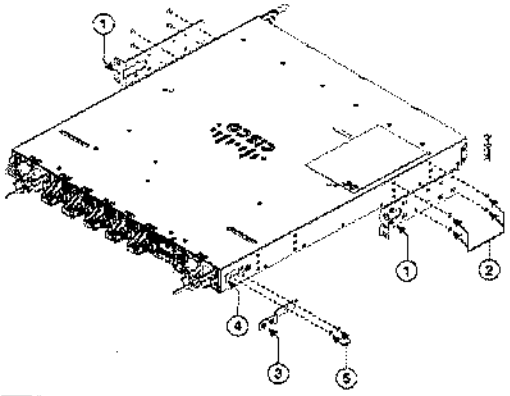


Figure 10: Figure 8: Rack-Mount Brackets on Cisco 8201 Router—Port-Side Exhaust



1	Rack-mount brackets	4	Remove grounding cover (also)
2	M4 x 6-mm Phillips flat-head screws	5	M4 x 6-mm Phillips flat-head screws
3	Grounding plate		

Figure 11: Rack-Mount Brackets on Cisco 8201 Routers—Port-Side Intake

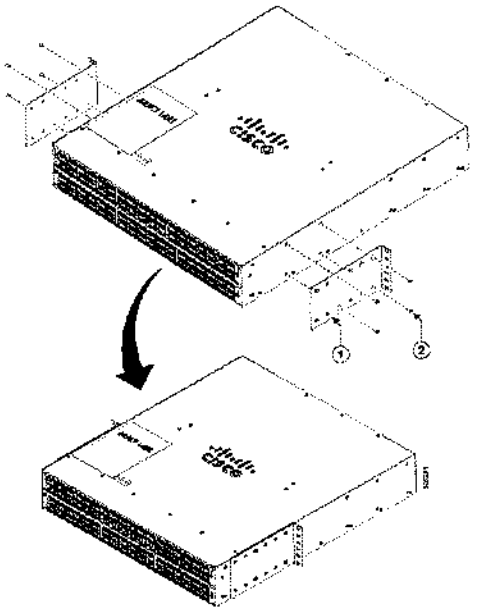
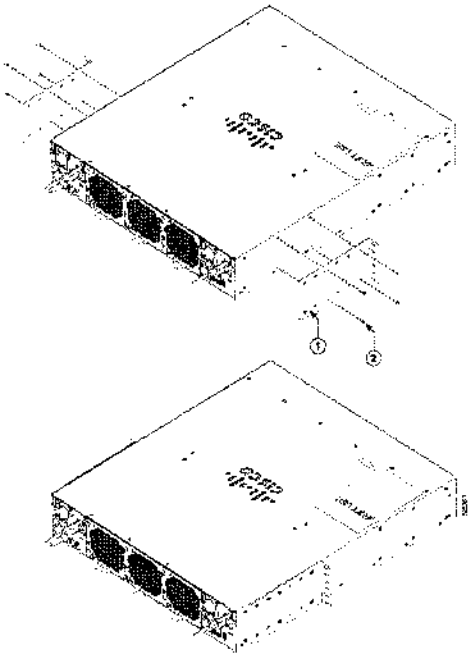


Figure 12: Rack-Mount Brackets on Cisco 8201 Router—Port-Side Exhaust



1	Rack-mount brackets	2	M4 x 6-mm Phillips flat-head screws

d) Repeat Steps 1b and 1c with the other rack-mount bracket on the other side of the router.

Step 2 Install the router onto the 2-post rack:

a) With the assistance of another person, lift the router into position between the two rack posts.
b) Move the router until the rack-mount brackets come in contact with two rack posts.
c) Hold the chassis at a level position while the second person inserts two screws (12-24 or 10-32, depending on the rack type) in each of the two rack-mount brackets (a total of four screws) and into the cage nuts or threaded holes in the vertical rack-mounting rails.
d) Tighten the 10-32 screws to 20 in-lb (2.26 N.m) or tighten the 12-24 screws to 30 in-lb (3.39 N.m).

Install the Air Filter

Air filters are used only on Cisco 8202 chassis which comes with a preinstalled air filter for port side intake configuration. For port side exhaust configuration, users must order the air filter kit FILTER-2RU-PE separately.

Note In general, we recommend that you inspect the air filter every three months and replace, if necessary, every six months.

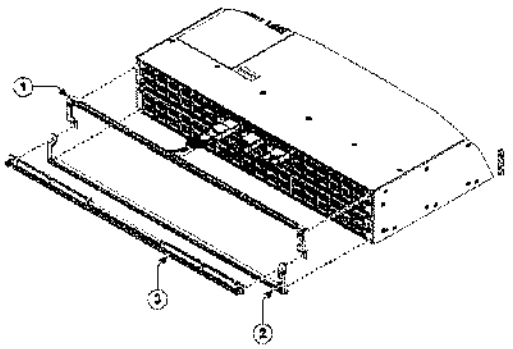
Install the Air Filter on the Port Side Inlet

If the air filter on the port-side inlet needs replacement, follow this procedure.

Note To fix the top and bottom filters use a manual screwdriver to gently turn the screws. Ensure that you turn the screws only three to four times, and that you do not overtighten the screws.

Step 1 Place the top air filter section on the top port-side of the chassis and secure it with the two screws at the upper left and right.

Figure 13: Port-side Intake Air Filter



1	Top Air Filter Section	3	Air Filter
2	Bottom Air Filter Section		

Step 2 Place the bottom air filter section along the bottom port-side of the chassis and secure it with the two screws at the lower left and right.

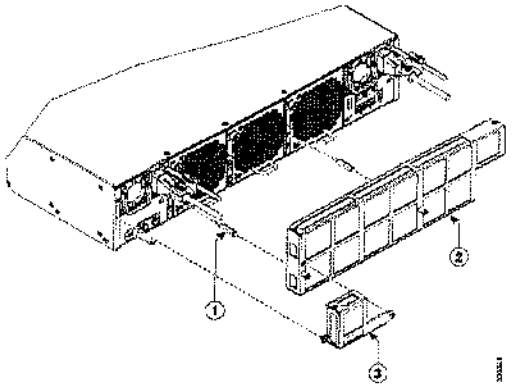
Step 3 Insert the air filter between the top and bottom air filter sections and tighten the six screws (two on each side, and two in the middle).

Install the Air Filter on the Port Side Exhaust

If the air filter on the port-side exhaust needs replacement, follow this procedure.

Step 1 Install the two standoffs to the chassis.

Figure 14: Port Side Exhaust Air Filter



1	Standoffs	3	Side Filter Extension
2	Main Air Filter		

Step 2 Install the main air filter by aligning it to the standoffs and tightening the two thumb screws.

Step 3 Install the side filter extension and tighten the 2 screws (1 to the chassis and 1 to the main air filter).

Ground the Chassis

Warning **Statement 1024**

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Warning **Statement 1046**

When installing or replacing the unit, the ground connection must always be made first and disconnected last.

Warning **Statement 1025**

Use copper conductors only.

Caution Grounding the chassis is required, even if the rack is already grounded. A grounding pad with two threaded holes is provided on the chassis for attaching either a grounding lug or grounding plate. The ground lug must be NRTL-listed. In addition, a copper conductor (wires) must be used and the copper conductor must comply with NEC code for ampacity.

Caution When terminating the frame ground, do not use soldering lug connectors, screwless (push-in) connectors, quick connect connectors, or other friction-fit connectors.

Step 1 Use a wire-stripping tool to remove approximately 0.75 inches (19 mm) of the covering from the end of the #6 AWG grounding cable.

Step 2 Insert the stripped end of the grounding cable into the open end of the grounding lug.

Step 3 Use the crimping tool to secure the grounding cable in the grounding lug.

Step 4 Attach the ground cable:

- Attach one end of the shelf ground cable (#6 AWG cable) to the grounding plate using the specified dual-hole lug connector.

Figure 15: Cisco 8201 Router Ground Lug

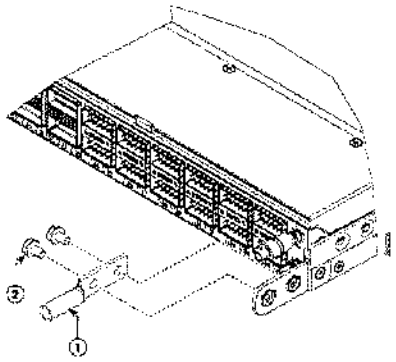
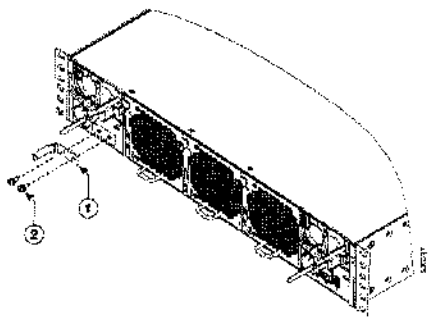


Figure 16: Cisco 8202 Router Ground Lug



1	Grounding lug	2	M4 x 6mm pan-head screws

Step 5 Tighten the pan-head screws to torque value of 11.5 in-lbs (1.3 N-m).

Step 6 Ensure that the lug and cable do not interfere with other equipment.

Step 7 Prepare the other end of the grounding cable, and connect it to an appropriate grounding point in your site to ensure adequate earth ground.

Connect AC Power to the Chassis

Caution The chassis relies on the protective devices in the building installation to protect against short circuit, overcurrent, and ground faults. Ensure that the protective devices comply with local and national electrical codes.

Note **Cisco 8201 Router**—Supports 1450W and 2000W PSU. For AC input source, router supports output power of 1450 W and 2000 W at high line voltage range 200Vac to 240Vac. To support low line applications, a voltage range between 100 Vac to 127 Vac is supported with maximum output power of 1000 W.

To provide full output power of 1450 W and 2000 W, the nominal voltage rating value ranges between 200 Vac to 240 Vac, depending on the standards in various countries.

Note **Cisco 8202 Router**—Supports 2000W PSU. For AC input source, router supports output power of 2000 W at high line voltage range 200Vac to 240Vac. To support low line applications, a voltage range between 100 Vac to 127 Vac is supported with maximum output power of 1000 W. To provide full output power of 2000 W, the nominal voltage rating value ranges between 200Vac to 240Vac, depending on the standards in various countries.

The following combinations of power supplies are supported:

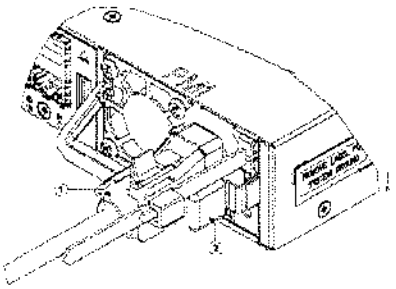
- PSU2KW-ACPI/PSU2KW-ACPI=, port-side intake airflow
- PSU2KW-ACPE/PSU2KW-ACPE=, port-side exhaust airflow
- PSU1.4KW-ACPI/PSU1.4KW-ACPI=, port-side intake airflow
- PSU1.4KW-ACPE/PSU1.4KW-ACPE=, port-side exhaust airflow

Note A dual pole breaker is needed for installation. For determining the recommended breaker size, pl[illegible]ere to local and national rules and regulations. The breaker size is based on the specifications of the [illegible] or the current drawn and the specified voltage level.

Step 1 Verify that the AC cable is installed in the correct AC source and outlet type.

Step 2 Attach the AC power cable to the cable connector in the AC power module.
Step 3 Place the cable through the opening in the cable clamp.
Step 4 Slide the cable clamp toward the plug.
Step 5 Close the cable clamp on the shoulder of the power cable to secure the power cable.

Figure 17: Connecting AC Power



1	AC power cable	2	Cable clamp

Power Supply Unit Input and Output Ranges

This table summarizes input and output power ranges for PSU low line and nominal applications:

Table 5: Input and output power ranges for PSUs

PID	Input Voltage	Input Current (Max)	Output Power	Output
PSU1.4KW-ACPI For low line applications	100-127V ac	12A	1000W	12V/84A
PSU1.4KW-ACPI For nominal voltage application	200-240V ac	9A	1450W	12V/121A
PSU1.4KW-ACPE For low line applications	100-127V ac	12A	1000W	12V/84A

PID	Input Voltage	Input Current (Max)	Output Power	Output
PSU1.4KW-ACPE For nominal voltage application	200-240V ac	9A	1450W	12V/121A
PSU2KW-ACPI For low line applications	100-127V ac	12A	1000W	12V/84A
PSU2KW-ACPI For nominal voltage application	200-240V ac	12A	2000W	12V/167A
PSU2KW-ACPE For low line applications	100-127V ac	12A	1000W	12V/84A
PSU2KW-ACPE For nominal voltage application	200-240V ac	12A	2000W	12V/167A
PSU2KW-DCPI	-40V - -72V DC	40A	2000W	12V/167A
PSU2KW-DCPE	-40V - -72V DC	40A	2000W	12V/167A
For high line applications	180V - 264V AC	9 A	1450W	
For low line applications	90V - 140V AC	12A	1000W	
For high line applications	180V - 264V AC	12 A	2000W	

Connect DC Power to the Chassis

Caution The chassis relies on the protective devices in the building installation to protect against short circuit, overcurrent, and ground faults. Ensure that the protective devices comply with local and national electrical codes.

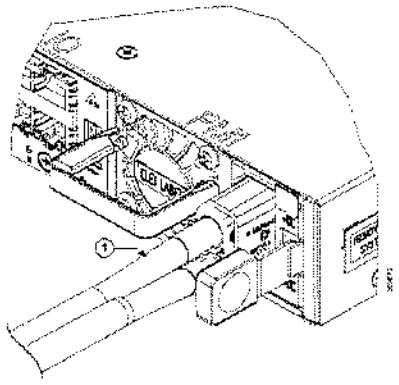
Note The supported output DC power is 2000 W. To provide full output power of 2000 W, the nominal voltage rating value ranges between -40 V to -72 V, depending on the standards in various countries.

The following combinations of power supplies are supported:

- PSU2KW-DCPI/PSU2KW-DCPI-, port-side intake airflow
- PSU2KW-DCPE/PSU2KW-DCPE-, port-side exhaust airflow

Verify that the correct fuse panel is installed in the top mounting space.
Ensure that the DC circuit is powered down (either breaker turned off or fuse pulled) and proper lockout/tag out procedures are followed. Use the cable (PID: 72-100992-02) supplied with the power supply. If you prefer to use your own cable, the cable size must be 6 AWG.
Step 3 Dress the power according to local practice.
Step 4 Connect the office battery and return cables according to the fuse panel engineering specifications.
Step 5 Insert the DC connector into the DC receptacle on the power supply.

Figure 18: Connecting DC Power



1	DC power cable

Step 6 Ensure that the locking mechanism has engaged to secure the cable.
Turn on the circuit breaker at the power source.

CHAPTER 4

Connect Router to the Network

Port Connection Guidelines

Depending on the chassis , you can use optical modules and RJ-45 connectors to connect the ports to other network devices.

To prevent damage to the fiber-optic cables, we recommend that you keep the transceivers disconnected from their fiber-optic cables when installing the transceiver in the line card. Before removing a transceiver from the router, remove the cable from the transceiver.

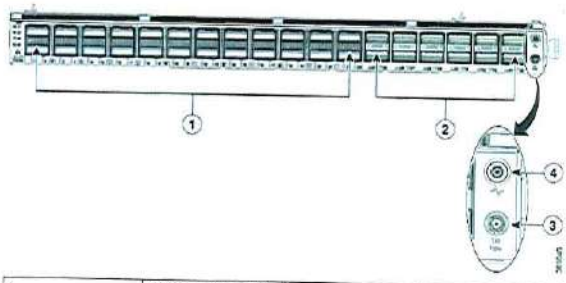
To maximize the effectiveness and life of your transceivers and optical cables, ensure the following:

- Wear an ESD-preventative wrist strap that is connected to an earth ground whenever you handle transceivers.
- Do not remove and insert a transceiver more often than is necessary. Repeated removals and insertions can shorten its useful life.
- Keep the transceivers and fiber-optic cables clean and dust free to maintain high signal accuracy and to prevent damage to the connectors. Attenuation (loss of light) is increased by contamination and should be kept below 0.35 dB.
  - Clean these parts before installation to prevent dust from scratching the fiber-optic cable ends.
  - Clean the connectors regularly; the required frequency of cleaning depends upon the environment. In addition, clean connectors when they are exposed to dust or accidentally touched. Both wet and dry cleaning techniques can be effective; refer to your site's fiber-optic connection cleaning procedures.

- Do not touch the ends of connectors. Touching the ends can leave fingerprints and cause dirt contamination.
- Inspect routinely for dust and damage. If you suspect damage, clean and then inspect fiber ends under a microscope to determine if damage has occurred.

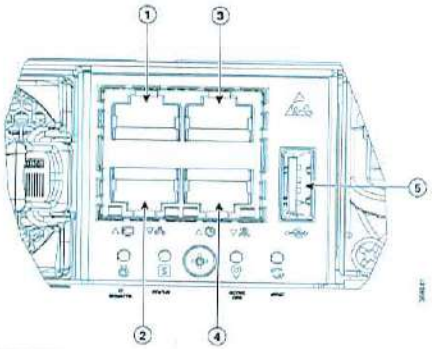
Interfaces and Port Description

Figure 19: Cisco 8201 Fixed Port Router - Front View



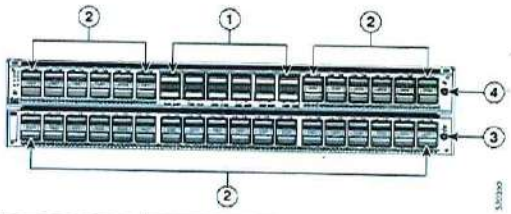
1	400G Ports (Port 0 to Port 23). 400G port supports 40GE, 100GE, 200GE, and 400GE. All 400G port support breakout operation.	3	Mini coax connector for 10MHz, input, and output.
2	100G ports (Port 24 to Port 35) support 100G and 40G. Ports 24, 26, 28, 30, 32, and 34 support 4x10G and 4x50G via breakout cable.	4	Mini coax connector for 1 PPS, input, and output.

Figure 20: Cisco 8201 Fixed Port Router - Rear View



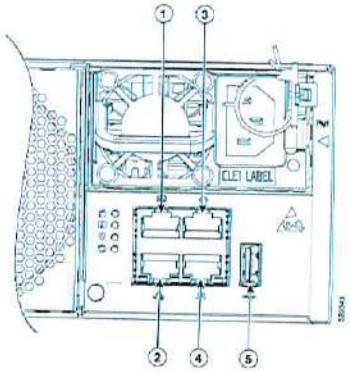
1	Console Port	4	1000BASE-T Management and BMC (Baseboard Management Controller) Port
2	10GBASE-T Control Plane Expansion Port	5	USB Port Type-A
3	RJ-45 connector for Time-of-Day (TOD) interface, input, and output		

Figure 21: Cisco 8202 Fixed Port Router - Front View



1	400G Ports. All 400G port support breakout operation.	3	1.0/2.3 50 ohm connector for 10MHz, input, and output.
2	100G ports and even ports support 4x10G and 4x50G	4	1.0/2.3 50 ohm connector for 1 PPS, input, and output.

Figure 22: Cisco 8202 Fixed Port Router - Rear View



1	Console Port	4	1000BASE-T Management and BMC (Baseboard Management Controller) Port
2	100GBASE-T Control Plane Expansion Port	5	USB Port Type-A
3	RJ-45 connector for Time-of-Day (TOD) interface, input, and output		

Transceiver and Cable Specifications

To determine which transceivers and cables are supported by this router, refer to the Transceiver Module Group (TMG) Compatibility Matrix Tool:

https://tmgmatrix.cisco.com/home

- For QSFP-DD data sheets, refer to the Cisco 400G QSFP-DD Cable and Transceiver Modules Data Sheet.
- For QSFP28 data sheets, refer to the Cisco 100GBASE QSFP-100G Modules Data Sheet.
- For QSFP+ data sheets, refer to the Cisco 40GBASE QSFP Modules Data Sheet.

PID	Distance, media (connector)
QSFP-DD Transceiver Modules	
QDD-400G-CU1M	1m passive copper cable
QDD-400G-CU2M	2m passive copper cable
QDD-400-CU2.5M	2.5m passive copper cable
QDD-400-CU3M	3m passive copper cable
QDD-400G-FR4	2km duplex SMF (LC)
QDD-400G-LR8	10km duplex SMF (LC)
QDD-400G-DR4-S	500m parallel SMF (MPO-12)
QDD-2x100G-CWDM4	2km dual duplex SMF (CS)
QDD-2x100G-SR4	100m MMF ribbon (MPO-24)
QSFP28 Transceiver Modules (Data sheet)	
QSFP-100G-FR-S	2km over SMF (LC)
QSFP-100G-ER4L-S	40km reach over SMF
QSFP-100G-LR4-S	10km over SMF (LC)

PID	Distance, media (connector)
QSFP-100G-CWDM4-S	2km over SMF (LC)
QSFP-100G-SR4-S	100m over OM4 MMF (MPO-12)
QSFP-100G-SM-SR	2km over SMF (LC)
QSFP+ Transceiver Modules (Data sheet)	
QSFP-40G-SR4 (4x10G and 4x50G breakout only on even-numbered ports)	100m/150m, MMF (MPO-12)
QSFP-4x10-LR-S (supported on even-numbered ports)	10km, SMF (MPO-12)

Connecting a Console to the Router

Before you create a network management connection for the router or connect the router to the network, you must create a local management connection through a console terminal and configure an IP address for the router. The router can be accessed using remote management protocols, such as SSH, Telnet, SCP and FTP. By default, SSH is included in the software image. But telnet is not part of the software image. You must manually install the telnet optional package to use it.

You also can use the console to perform the following functions, each of which can be performed through the management interface after you make that connection:

- configure the router using the command-line interface (CLI)
- monitor network statistics and errors
- configure Simple Network Management Protocol (SNMP) agent parameters
- initiate software download updates via console

You make this local management connection between the asynchronous serial port on a console device capable of asynchronous transmission. Typically, you can use a computer terminal as the console device.

Note Before you can connect the console port to a computer terminal, make sure that the computer terminal supports VT100 terminal emulation. The terminal emulation software makes communication between the router and computer possible during setup and configuration.

Before you begin

- The router must be fully installed in its rack. The router must be connected to a power source and grounded.
- The necessary cabling for the console, management, and network connections must be available.
  - An RJ45 rollover cable and a DB9F/RJ45 adapter.
  - Network cabling should already be routed to the location of the installed router.

Step 1 Configure the console device to match the following default port characteristics:

- 115200 baud
- 8 data bits
- 1 stop bit
- No parity

Step 2 Connect and RJ45 rollover cable to a terminal, PC terminal emulator, or terminal server.

You can find this cable in the accessory kit.

Step 3 Route the RJ45 rollover cable as appropriate and connect the cable to the console port on the chassis.

If the console or modem cannot use an RJ45 connection, use the DB9F/RJ45F PC terminal adapter. Alternatively, you can use an RJ45/DSUB F/F or RJ45/DSUB R/P adapter, but you must provide those adapters.

What to do next

You are ready to create the initial router configuration.

Create the Initial Router Configuration

You must assign an IP address to the router management interface to connect the router to the network.

When you initially power up the router, it boots up and asks a series of configuration-related questions. You can use the default choices for each configuration except for the IP address, which you must provide.

When the system is powered on and the console port is connected to the terminal, the RP CPU messages are seen. You can toggle between BMC CPU messages and RP CPU messages by pressing the hot-key sequence Ctrl-O.

To configure IP address for Ethernet port on BMC and other additional information related to BMC, please see the *System Setup Guide for Cisco 8000 Series Routers*.

Before you begin

- A console device must be connected with the router.
- The router must be connected to a power source.
- Determine the IP address and netmask that is needed for the Management interfaces: MgmtEth0/[illegible]/CPU0/0 :

Step 1 Power up the router.

The LEDs on each power supply light up (green) when the power supply units are sending power to the router, and the software asks you to specify a password to use with the router.

Step 2 When the system is booted up for the first time, a new username and a password is to be created. The following prompt appears:

```
!!!!!!!!!!!!!!!!! No root-system username is configured. Need to configure root-system username. !!!!!!!!!!!!!!!!!

--- Administrative User Dialog ---


Enter root-system username:
% Entry must not be null.

Enter root-system username: cisco
Enter secret:
Use the 'configure' command to modify this configuration.
User Access Verification

Username: cisco
Password:


RP/0/RP0/CPU0:ios#
```

Step 3 Enter a new password to use for this router.

The software checks the security strength of your password and rejects your password if it is not considered to be a strong password. To increase the security strength of your password, make sure that it adheres to the following guidelines:

- at least eight characters
- minimizes or avoids the use of consecutive characters (such as "abcd")
- minimizes or avoids repeating characters (such as "aaa")
- does not contain recognizable words from the dictionary
- does not contain proper names
- contains both uppercase and lowercase characters
- contains numbers as well as letters

Note Clear text passwords cannot include the dollar sign ($) special character.

Tip If a password is trivial (such as a short, easy-to-decipher password), the software rejects that password. Passwords are case sensitive.

When you enter a strong password, the software asks you to confirm the password.

Step 4 Reenter the password.

When you enter the same password, the software accepts the password.

Step 5 Enter the configuration mode.

Step 6 Enter the IP address for the management interface.

Step 7 Enter a network mask for the management interface.

Step 8 The software asks whether you want to edit the configuration. Enter 'no' to decline.

Connect the Management Interface

The management port (MGMT ETH) provides out-of-band management, which lets you to use the command-line interface (CLI) to manage the router by its IP address. This port uses a 100/1000 Ethernet connection with an RJ-45 interface.

Caution To prevent an IP address conflict, do not connect the MGMT 100/1000 Ethernet port until the initial configuration is complete.

Before you begin

You must have completed the initial router configuration.

Step 1 Connect a modular, RJ-45, UTP cable to the MGMT ETH port .
Step 2 Route the cable through the central slot in the cable management system.
Step 3 Connect the other end of the cable to a 100/1000 Ethernet port on a network device.

What to do next

You are ready to connect the interface ports to the network.

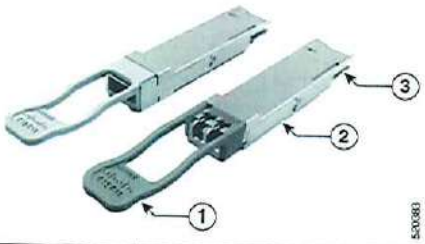
Install and Remove Transceiver Modules

Install and Remove QSFP Transceiver Modules

This section provides the installation, cabling, and removal instructions for the Quad Small Form-Factor Pluggable transceiver modules. Refer to the *Cisco Optical Transceiver Handling Guide* for additional details on optical transceivers.

The following figure shows a 400-Gigabit QSFP-DD optical transceiver.

Figure 23: 400-Gigabit QSFP-DD Transceiver Module



1	Pull-tab	2	QSFP-DD transceiver body
3	Electrical connection to the module circuitry		

Warning **Statement number—1092**Hot surface for Field Replaceable Units

Hot surface. Use care when handling.

Required Tools and Equipment

You need these tools to install the transceiver modules:

- Wrist strap or other personal grounding device to prevent ESD occurrences.
- Antistatic mat or antistatic foam to set the transceiver on.
- Fiber-optic end-face cleaning tools and inspection equipment.

Installing the Transceiver Module

Warning **Statement number—1092**Hot surface for Field Replaceable Units

Hot surface. Use care when handling.

Caution The transceiver module is a static-sensitive device. Always use an ESD wrist strap or similar individual grounding device when handling transceiver modules or coming into contact with system modules.

Caution Protect the transceiver ports by inserting clean dust caps (80000-QSFP-DCAP) into any ports not in use. Be sure to clean the optic surfaces of the fiber cables before you plug them back into the optical ports of another module.

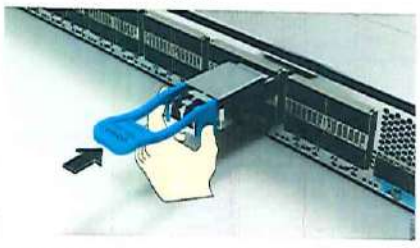
The router ships with dust caps plugged in. We highly recommend you to keep the dust caps plugged in until you are ready to plug an optic.

The dust caps protect the ports from possible EMI interference and also avoid contamination due to dust collection.

The QSFP transceiver module has a pull-tab latch. To install a transceiver module, follow these steps:

Step 1 Attach an ESD wrist strap to yourself and a properly grounded point on the chassis or the rack.
Step 2 Remove the transceiver module from its protective packaging.
Step 3 Check the label on the transceiver module body to verify that you have the correct model for your network. Do not remove the dust plug until you're ready to attach the network interface cable. Dust plug is not shown in the images.
Step 4 Hold the transceiver by the pull-tab so that the identifier label is on the top.
Step 5 Align the transceiver module in front of the module's transceiver socket opening and carefully slide the transceiver into the socket until the transceiver contact with the socket electrical connector.

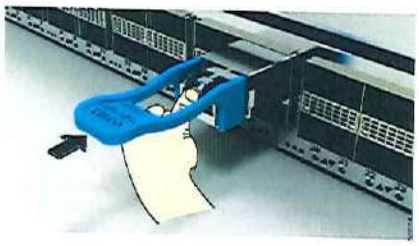
Figure 24: Installing the QSFP Transceiver Module



Step 6 Press firmly on the front of the transceiver module with your thumb to fully seat the transceiver in the module's transceiver socket (see the below figure).

Caution If the latch isn't fully engaged, you might accidentally disconnect the transceiver module.

Figure 25: Seating the QSFP Transceiver Module



Attach the Optical Network Cable

Before you begin

Before you remove the dust plugs and make any optical connections, follow these guidelines:

- Keep the protective dust plugs installed in the unplugged fiber-optic cable connectors and in the transceiver optical bores until you are ready to make a connection.
- Inspect and clean the MPO connector end faces just before you make any connections.
- Grasp the MPO connector only by the housing to plug or unplug a fiber-optic cable.

Note The transceiver modules and fiber connectors are keyed to prevent incorrect insertion.

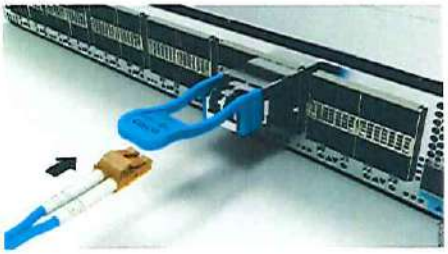
Note The multiple-fiber push-on (MPO) connectors on the optical transceivers support network interface cables with either physical contact (PC) or ultra-physical contact (UPC) flat polished face types. The MPO connectors on the optical transceivers do not support network interface cables with an angle-polished contact (APC) face type.

Note Inspect the MPO connector for the correct cable type, cleanliness, and any damage. For complete information on inspecting and cleaning fiber-optic connections, see the *Inspection and Cleaning Procedures for Fiber-Optic Connections* document.

Step 1 Remove the dust plugs from the optical network interface cable MPO connectors and from the transceiver module optical bores. Save the dust plugs for future use.

Step 2 Attach the network interface cable MPO connectors immediately to the transceiver module.

Figure 20: Cabling a Transceiver Module



Removing the Transceiver Module

Caution The transceiver module is a static-sensitive device. Always use an ESD wrist strap or similar individual grounding device when handling transceiver modules or coming into contact with modules.

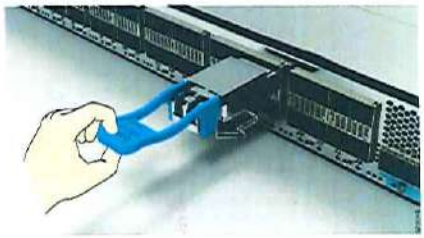
To remove a transceiver module, follow these steps:

S Disconnect the network interface cable from the transceiver connector.

St Install the dust plug immediately into the transceiver's optical bore.

Step 3 Grasp the pull-tab and gently pull to release the transceiver from the socket.

Figure 21: Removing the QSFP Transceiver Module



Step 4 Slide the transceiver out of the socket.

Step 5 Place the transceiver module into an antistatic bag.

Connect Interface Ports

You can connect optical interface ports with other devices for network connectivity.

Connect a Fiber-Optic Port to the Network

40G, 100G, 2x100G, or 400G transceivers are supported on Cisco 8200 series routers. Some transceivers work with fiber-optic cables that you attach to the transceivers and other transceivers work with pre-attached copper cables. You must install a transceiver in the port before installing the fiber-optic cable in the transceiver.

Caution Removing and installing a transceiver can shorten its useful life. Do not remove and insert transceivers any more than is absolutely necessary. We recommend that you disconnect cables before installing or removing transceivers to prevent damage to the cable or transceiver.

Disconnect Optical Ports from the Network

When you need to remove fiber-optic transceivers, you must first remove the fiber-optic cables from the transceiver before you remove the transceiver from the port.

Maintain Transceivers and Optical Cables

Refer to Inspection and Cleaning Procedures for Fiber-Optic Connections document for inspection and cleaning processes for fiber optic connections.

Verify Chassis Installation

After installing the chassis, use the following show commands to verify the installation and configuration in the EXEC mode.If you detect any issues, take corrective action before making further configurations.

Command	Description
show platform	Displays the operational status of the node.
show inventory	Displays information about the field replaceable units (FRUs), including product IDs, serial numbers, and version IDs.
show environment	Displays all the environment-related router information.
show environment temperature	Displays temperature readings from the various sensors on the router. Each system controller has temperature sensors with two thresholds: • Minor temperature threshold – When a minor threshold is exceeded, a minor alarm occurs and the following actions occur for all temperature thresholds: • displays system messages • sends SNMP notifications (if configured) • log environmental alarm event that can be reviewed by running the **show alarms** command. Users can use the **show alarms brief system active** command to verify active alarms in the system. • Major temperature threshold – When a major threshold is exceeded, a major alarm occurs and the following actions occur: • displays system messages • sends SNMP notifications (if configured) • log environmental alarm event that can be reviewed by running the **show alarms** command. Users can use the **show alarms brief system active** command to verify active alarms in the system. • Critical temperature threshold – When a critical threshold is exceeded, a critical alarm occurs and the following actions occur: • displays system messages. • sends SNMP notifications (if configured). • logs environmental alarm event that can be reviewed by running the **show alarms** command. Users can use the **show alarms brief system active** command to verify active alarms in the system. • triggers a chassis shutdown.
show environment power	Displays power usage information for entire router.

Command	Description
show environment voltage	Displays voltage for entire router.
show environment current	Displays current reading from various sensors.
show environment fan	Displays status of fan trays.
show media	Displays media information of the node.

CHAPTER 5

Replace Chassis Components

Replace Fan Modules for Cisco 8201 Routers

The fan module is designed to be removed and replaced while the system is operating without presenting an electrical hazard or damage to the system. Please keep the replacement fan modules ready prior to attempting this task.

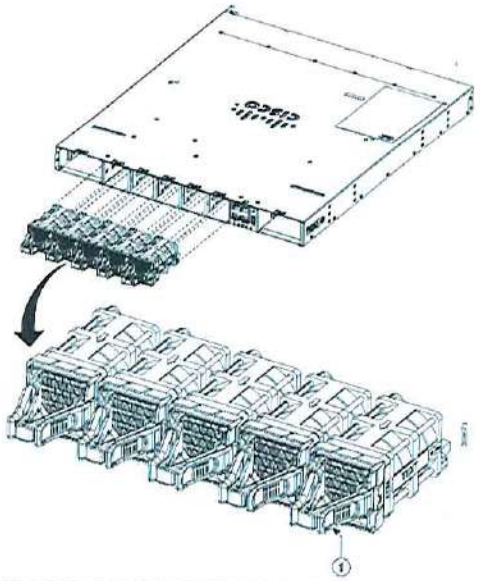
Note The routers support FAN-1RU-PI (port-side intake airflow) and FAN-1RU-PE (port-side exhaust airflow) fan modules.

Note The airflow direction must be the same for all power supply and fan modules in the chassis.

Step 1 To remove a fan module, follow these steps:

a) Press two latches on the fan module and grasp the handle of fan module.

Figure 28: Cisco 8201 Router — Remove Fans



1	Latched fan module

b) As you simultaneously press the latches pull the fan module fully out of the chassis.

Step 2 To install a fan module, follow these steps:

a) Hold the fan module with the LED at the top.

b) Align the fan module to the open fan tray slot in the chassis, and press the module all the way into the slot until the left and right latches click and are locked on the chassis.

Note If the fan module does not go all the way into the slot, do not force it. Remove the fan module and verify that it is the correct type for your router and in the correct orientation. To verify the status of fans and the speed, use the **show environment fan** command.

c) If the chassis is powered on, listen for the sound of the fans in operation. You should immediately hear them in operation. If you do not hear them, ensure that the fan module is inserted completely in the chassis.

Note During the fan module replacement, the other fans adjust their speed to allow for proper initialization of the new module. When you insert a new fan module, the fans may run at lower or higher speeds for a few minutes.

d) Verify that the fan module LED is green. If the LED is not green, one or more fans are faulty. If this situation occurs, contact your customer service representative for replacement parts.

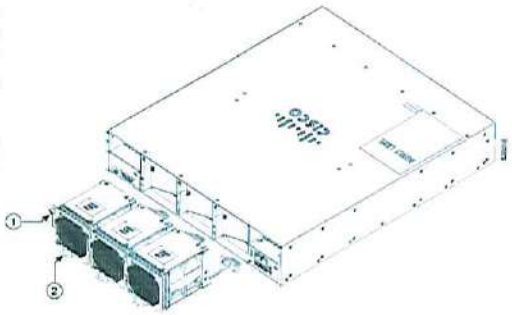
Replace Fan Modules for Cisco 8202 Routers

The fan module is designed to be removed and replaced while the system is operating without presenting an electrical hazard or damage to the system. Please keep the replacement fan modules ready prior to attempting this task.

Note The airflow direction must be the same for all power supply and fan modules in the chassis.

Step 1 Unscrew the thumbscrew on the fan.

Figure 29: Remove Cisco 8202 Fan Modules



1	Fan module thumbscrew	2	Handle

Step 2 Pull the handle to remove the fan to be replaced.

Step 3 Hold the fan module with the LED and PID label at the top.

Step 4 Align the fan module to the open fan slot in the chassis and press the module all the way into the slot until the front of the fan module touches the chassis.

Make sure that the thumbscrew on the fan module is aligned with the screw hole in the chassis.

Step 5 Tighten the thumbscrew to secure the fan module in the chassis.

Step 6 If the chassis is powered on, listen for the fans. You should immediately hear them operating. If you do not hear them, ensure that the fan module is inserted completely in the chassis.

Step 7 Verify that the fan module LED is green. If the LED is not green, one or more fans are faulty. If this situation occurs, contact your customer service representative for replacement parts.

Replace Power Supply

Use this procedure to replace the AC or DC power supply units. Be sure to power down the fixed configuration PDU (power distribution unit) before removing it from the chassis.

Step 1 If the power supply is connected to a AC or DC circuit, shut off the circuit at the circuit breaker.

Step 2 Disconnect the PSU cable.

Step 3 Press the tab inward to unlatch the PSU, and pull the handle to remove the PSU.

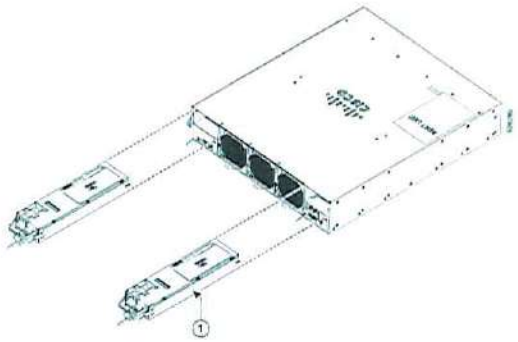
Step 4 Insert the new PSU.

Note If the PSU does not go all the way into the slot, do not force it. Remove the PSU and verify that it is the correct type for your router and in the correct orientation.

Step 5 Connect the PSU cable.

Step 6 If the power supply is connected to a AC or DC circuit, turn on the circuit breaker for the AC or DC power source. After replacing the PSU, verify the power using the **show environment power** command.

Figure 30: Cisco 8202 Router — Remove Power Supply



CHAPTER 6

LEDs

Chassis LEDs

Attention, Status, Synchronization, and GPS LEDs are located both at the far left of the front of the chassis and also on the back of the chassis:

Figure 31: Chassis LEDs - Front View of Cisco 8201 Chassis

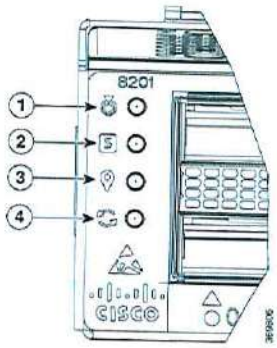


Figure 32: Chassis LEDs - Rear View of Cisco 8201 Chassis

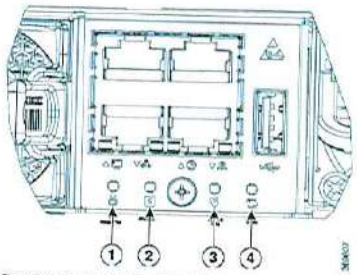
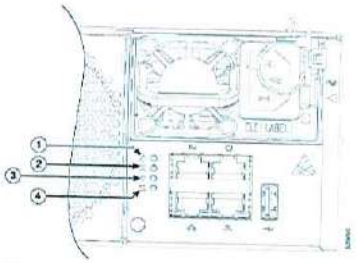


Figure 33: Chassis LEDs - Rear View of Cisco 8202 Chassis



1	Attention	3	GPS
2	Status	4	Synchronization

Table 6: Chassis LED Descriptions

LED	Color	Status
Attention	Flashing blue	The operator has activated this LED to identify this chassis.
	Off	This chassis is not being identified.

LED	Color	Status
Status	Green	The module is operational and has no active major or critical alarms.
	Flashing Green	The auto or manual FPD upgrade is in progress.
	Amber	The module is in one of the following states: • Power cycle • Reload or reimage • Shutdown
	Flashing Amber	The module has minor alarm.
	Red	Power-up failure which prevents the CPU from booting.
	Flashing Red	The module has active major or critical alarms.
	Off	The module is powered-off.
Synchronization	Green	Time core is synchronized to an external source including IEEE1588.
	Amber	The system is running in holdover or free-run mode and it is not synchronized to an external interface.
	Off	The centralized frequency or time and phase distribution is not enabled.
GPS	Green	The GPS interface is provisioned and frequency, time of day and phase inputs are all operating correctly.
	Off	The GPS interface is not provisioned, or the GPS inputs are not working correctly.

Fan Tray LED

Fan tray modules are located on the back of the chassis. Each fan tray module has a Status LED.

Figure 34: Fan Tray LED - Cisco 8201 Chassis

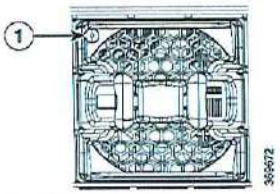
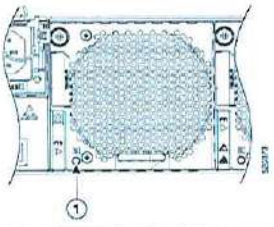


Figure 35: Fan Tray LED - Cisco 8202 Chassis

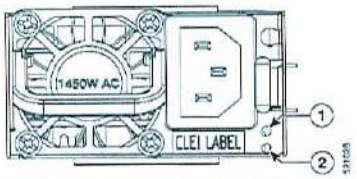


LED	Color	Status
STATUS	Green	Fan is operating normally.
	Amber	Fan tray is inserted and pending to come online.
	Flashing Amber	Fan has failed.
	Off	Fan is not receiving power.

Power Supply LEDs

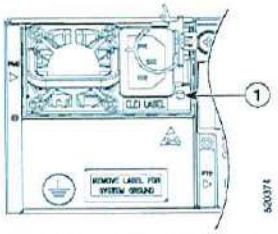
Power modules are located on the back side of the chassis. Each power module has a Status LED.

Figure 36: Power Supply LED - 1450W



1	Status LED
2	Attention LED

Figure 37: Power Supply LED - 2600W



1	Status LED

Table 7: Power Supply LED Descriptions

LED	Color	Status
STATUS	Green	Power supply is on and transmitting power to the router.
	Flashing Green	Power supply is connected to input power source but not tr... power to the router.
	Amber	Power supply failure, due to one of the following conditions: • Over voltage • Over current • Over Temperature • Fan failure
	Flashing Amber	Power supply is operating but a warning condition has occurred, due to one of the following conditions: • High temperature • High power • Slow fan
	Off	Power supply units are not receiving power.
Attention	Flasing Blue	The operator has activated this LED to identify this PSU.
	Off	This PSU is not being identified.

Port Status LEDs

Each port has an LED. The following table describes port status LEDs.

Figure 38: Port Status LED - Cisco 8201 Chassis

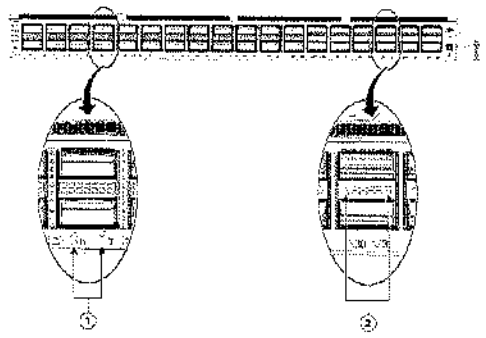
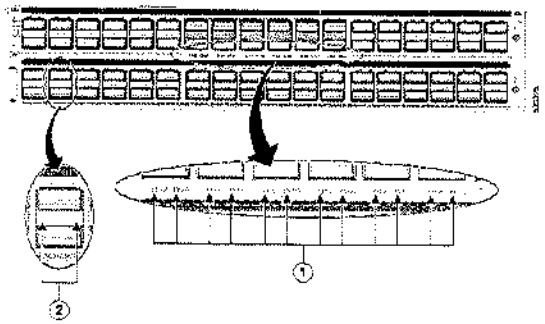


Figure 39: Port Status LED - Cisco 8202 Chassis



1	400G Port Status LED	2	100G Port Status LED

Table 8: Port Status LEDs (one per port)

LED Color	Description
Off	Port is administratively shut down.
Amber	Port is administratively enabled and the link is down.
Green	Port is administratively enabled and the link is up.